Exhibit A

US009096189B2

(12) **United States Patent**
Golden

(10) **Patent No.:** **US 9,096,189 B2**
(45) **Date of Patent:** **Aug. 4, 2015**

(54) **MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM**

(71) Applicant: **Larry Golden**, Mauldin, SC (US)

(72) Inventor: **Larry Golden**, Mauldin, SC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/021,693**

(22) Filed: **Sep. 9, 2013**

(65) **Prior Publication Data**

US 2014/0071274 A1 Mar. 13, 2014

Related U.S. Application Data

(60) Continuation of application No. 13/288,065, filed on Nov. 3, 2011, now Pat. No. 8,531,280, which is a division of application No. 12/802,001, filed on May 27, 2010, now Pat. No. 8,334,761, which is a continuation of application No. 12/657,356, filed on Jan. 20, 2010, now Pat. No. 8,106,752.

(51) **Int. Cl.**

B60R 25/10	(2013.01)
B60R 25/102	(2013.01)
B60R 25/01	(2013.01)
B60R 25/04	(2013.01)
G07C 9/00	(2006.01)
G08B 15/00	(2006.01)
G08B 21/12	(2006.01)

(52) **U.S. Cl.**
CPC ***B60R 25/102*** (2013.01); ***B60R 25/018*** (2013.01); ***B60R 25/04*** (2013.01); ***G07C 9/00912*** (2013.01); ***G08B 15/00*** (2013.01); ***G08B 21/12*** (2013.01); *B60R 2325/205* (2013.01); *B60R 2325/304* (2013.01); *G07C 2009/0092* (2013.01)

(58) **Field of Classification Search**
CPC ... B60R 2325/00; G08B 21/12; G08B 25/009
USPC 340/539.1, 539.11, 539.13, 539.16, 340/539.17, 539.22, 539.25, 539.26, 540, 340/573.1, 574; 348/143; 380/228, 229, 380/232; 382/103, 115; 702/32
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,385,469	A	5/1983	Scheuerpflug
4,544,267	A	10/1985	Schiller
4,586,441	A	5/1986	Zekich
4,792,226	A	12/1988	Fishbine
5,222,152	A	6/1993	Fishbine

(Continued)

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 11/397,118; mailed Nov. 14, 2007; Alexandria, Virginia, USA; pp. 1-12; parent U.S. Appl. No. 13/288,065 (12 pages).

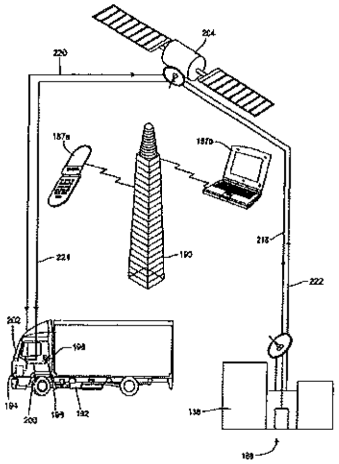
(Continued)

Primary Examiner — Van Trieu

(57) **ABSTRACT**

A multi sensor detection and disabling lock system includes detector cases for holding interchangeable detectors that sample for chemical, biological and radiological compounds, agents and elements, with each detector case disposed in or upon the monitored product. The detector case transmits detection information to a monitoring computer terminal and transmits a signal to a lock disabler engaged to the product to lock or disable the product's lock thereby preventing untrained, unauthorized and unequipped individual's from gaining access and entry to the product, and also preventing further contamination of the area. The detection system can be interconnected to surveillance towers scanning detector cases disposed at seaport docks, freight depots and rail terminals for monitoring containers being prepared for shipment or sitting on docks for long periods of time.

9 Claims, 13 Drawing Sheets



(56) References Cited

U.S. PATENT DOCUMENTS

5,223,844	A	6/1993	Mansell et al.	
5,233,404	A	8/1993	Lougheed	
5,557,254	A	9/1996	Johnson	
5,682,133	A	10/1997	Johnson	
5,766,956	A	6/1998	Groger	
5,938,706	A	8/1999	Feldman	
5,959,529	A	9/1999	Kail, IV	
5,963,657	A	10/1999	Bowker	
5,986,543	A	11/1999	Johnson	
5,990,785	A *	11/1999	Suda	340/426.21
6,049,269	A	4/2000	Byrd	
6,078,265	A	6/2000	Bonder	
6,262,656	B1	7/2001	Byrd	
6,271,745	B1	8/2001	Arizal	
6,374,652	B1	4/2002	Hwang	
6,411,887	B1	6/2002	Martens	
6,470,260	B2	10/2002	Martens	
6,542,076	B1	4/2003	Joao	
6,542,077	B2	4/2003	Joao	
6,588,635	B2	7/2003	Vor Keller	
6,610,977	B2	8/2003	Megerle	
6,613,571	B2	9/2003	Cordery	
6,628,813	B2	9/2003	Scott	
6,647,328	B2	11/2003	Walker	
6,738,697	B2	5/2004	Breed	
6,923,509	B1	8/2005	Barnett	
6,980,092	B2	12/2005	Turnbull	
6,988,026	B2	1/2006	Breed et al.	
7,005,982	B1	2/2006	Frank	
7,034,677	B2 *	4/2006	Steinthal et al.	340/539.12
7,034,683	B2	4/2006	Ghazarian	
7,103,460	B1	9/2006	Breed	
7,109,859	B2	9/2006	Peeters	
7,116,798	B1	10/2006	Chawla	
7,148,484	B2	12/2006	Craig et al.	
7,164,117	B2	1/2007	Breed et al.	
7,171,312	B2 *	1/2007	Steinthal et al.	702/32
7,243,945	B2	7/2007	Breed et al.	
7,339,469	B2	3/2008	Braun	
7,346,439	B2	3/2008	Bodin	
7,385,497	B2	6/2008	Golden	
7,397,363	B2	7/2008	Joao	
7,636,033	B2	12/2009	Golden	
7,647,180	B2	1/2010	Breed	
7,844,505	B1	11/2010	Arneson et al.	
7,868,912	B2 *	1/2011	Venetianer et al.	348/143
7,872,575	B2	1/2011	Tabe	
7,880,767	B2 *	2/2011	Chinigo	348/148
7,961,094	B2	6/2011	Breed	
8,274,377	B2	9/2012	Smith et al.	
8,531,521	B2 *	9/2013	Romanowich	348/143
8,564,661	B2 *	10/2013	Lipton et al.	348/143
2002/0145666	A1 *	10/2002	Scaman et al.	348/148
2003/0063004	A1 *	4/2003	Anthony et al.	340/574
2003/0137426	A1 *	7/2003	Anthony et al.	340/574
2003/0206102	A1	11/2003	Joao	
2004/0107028	A1	6/2004	Catalano	
2004/0222092	A1	11/2004	Musho	
2005/0195069	A1	9/2005	Dunand	
2006/0164239	A1	7/2006	Loda	
2006/0176169	A1 *	8/2006	Doolin et al.	340/521
2006/0181413	A1	8/2006	Mostov	
2006/0250235	A1	11/2006	Astrin	
2007/0171042	A1	7/2007	Metes et al.	
2008/0045156	A1	2/2008	Sakhpara	
2008/0122595	A1	5/2008	Yamamichi	
2008/0234907	A1	9/2008	Labuhn	
2010/0159983	A1	6/2010	Golden	
2011/0178655	A1	7/2011	Golden	

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action from U.S. 12/155,573; mailed Apr. 9, 2009; Alexandria, Virginia, USA; pp. 1-7; parent U.S. Appl. No. 13/288,065 (7 pages).

United States Patent and Trademark Office; Office Action from U.S. 12/155,573; mailed Jul. 30, 2009; Alexandria, Virginia, USA; pp. 1-9; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. 12/155,573; mailed Oct. 28, 2009; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/657,356; mailed Jul. 12, 2010; Alexandria, Virginia, USA; pp. 1-14; parent U.S. Appl. No. 13/288,065 (14 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. 12/657,356; mailed Mar. 10, 2011; Alexandria, Virginia, USA; pp. 1-4; parent U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 13/065,837; mailed Jul. 18, 2011; Alexandria, Virginia, USA, pp. 1-9; parent U.S. Appl. No. 13/288,065 (4 pages).

A newspaper article of Mr. Melvin Sullivan and his family that references the date, Mar. 6, 2001; parent U.S. Appl. No. 13/288,065.

A letter of response Mr. Sullivan received from Pfeiffer & Gantt, PA, dated Sep. 16, 2002; parent U.S. Appl. No. 13/288,065.

A "Certificate of Existance" Bright Idea Inventor, LLC. Nov. 6, 2002; parent U.S. Appl. No. 13/288,065.

Operating Agreement of Bright Idea Inventor, LLC received from Pfeiffer & Gantt, PA, dated Nov. 13, 2002; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Congressman from Maryland, Elijah E. Cummings, dated Dec. 16, 2002; parent U.S. Appl. No. 13/288,065.

A newspaper article of Mr. Melvin Sullivan and Mr. Larry Golden, dated, Feb. 27-Mar. 5, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated May 21, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Office of the Vice President, Dick Cheney, dated Jun. 3, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated Oct. 1, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Lindsey O. Graham, dated Oct. 21, 2003; parent U.S. Appl. No. 13/288,065.

A letter sent to the President of the United States George W Bush, the President's Cabinet, the United States Senate and the Congressional Black Caucus, dated May 23, 2005; parent U.S. Appl. No. 13/288,065.

On Nov. 17, 2005, an "Inventor's Official Record of Invention", was filed in my name (Golden) at "The Law Office of David P. Gaudio, P.C.; the Inventors Network."; parent U.S. Appl. No. 13/288,065.

On Aug. 23, 2005, the "Disclosure Document Registration"; parent U.S. Appl. No. 13/288,065.

On Apr. 5, 2006, the "Patent Application" was filed in my name (Golden) at the United Staets Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

On Jun. 6, 2008, the "Continuance-In-Part, (CIP) Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

On Jan. 20, 2010, a "Continuation Application" (U.S. Appl. No. 12/657,356) was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033;"Swear Back"; in accordance to Title 37—Code of Federal Regulations Patents, Trademarks, and Copyrights; Apr. 8, 2011; parent U.S. Appl. No. 13/288,065

Reissue of U.S. Pat. No. 7,636,033; "Swearback—History of Work"; Apr. 8, 2011; parent U.S. Appl. No. 13/288,065

United States Patent and Trademark Office; Office Action from U.S. 12/802,001; mailed Apr. 14, 2011; Alexandria, Virginia, USA; pp. 1-16; parent U.S. Appl. No. 13/288,065 (16 pages)

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed Oct. 20, 2011; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages).

(56) **References Cited**

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed May 27, 2011; Alexandria, Virginia, USA; pp. 1-14; parent U.S. Appl. No. 13/288,065 (14 pages)

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and mailing date Dec. 12, 2011, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action, Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Dec. 2, 2011, pp. 1-27, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (27 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Nov. 1, 2011, pp. 1-18, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (18 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and mailing date Jan. 13, 2012, pp. 1-34, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (34 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and mailing date Mar. 26, 2012, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and mailing date Feb. 22, 2012, pp. 1-38, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (38 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Feb. 22, 2012, pp. 1-25, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (25 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Aug. 24, 2012, pp. 1-4, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Nov. 28, 2012, pp. 1-11, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (11 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Apr. 16, 2013, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Department of Homeland Security; Petition for Inter Partes Review of U.S. Pat. No. Re. 43,990 Under 35 U.S.C. §312 and 37 C.F.R. §42.104; Case IP2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-57; (57 pages).

United States Department of Homeland Security; Declaration of Dr. Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-44; (44 pages).

Richard R Brooks and S.S. Iyengar; Multi-Sensor Fusion Fundamentals and Applications with Software; pubished 1998; Copyright Prentice Hall PTR; Upper Saddle River, New Jersey, USA; pp. 1-20; (20 pages).

Ramanarayanan Viswanathan and Pramod K Varshney; Distributed Detection with Multiple Sensors; Part 1—Fundamentals; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-11; vol. 85; No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; pp. 1-11; (11 pages).

Blum; Distributed with Multiple Sensors: Part II—Advanced Topics; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-16; vol. 85, No. 1; Southern Illinois University Carbondale Open SIUC; Illinois, USA, pp. 1-11; (16 pages).

Victor Lesser; Distributed Sensor Networks a Multiagent Perspective; 2003; pp. 1, 2, 5, 6, 22, 26, 27, 36, 275, 320; copyright 2003 Kluwer Academic Publishers: AH Dordrecht, The Netherlands; (10 pages).

Samuel Blackman and Robert Popoli; Design and Analysis of Modern Tracking Systems; 1999; pp. 1, 2, 6, 472; copyright 1999 Artech House; Norwood, Massachusetts, USA; (4 pages).

Jean-Francois Chamberland; Decentralized Detection in Sensor Networks; 2003; pp. 407-416; IEEE Transactions on SIgnal Processingl vol. 51, No. 2; Urbana, Illinois, USA; (10 pages).

Oleg Kachirski and Ratan Guha; Effective instrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks; pp. 1-8; Proceedings of the 36th Hawaii International Conference on System Sciences; copyright 2003; Orlando, Florida, USA; (8 pages).

Lawrence A Klein; Sensor and Data Fusion a Tool for Information Assessment and Decision Making; 2004; pp. 1-4, 6, 81, 87-89; copyright 2004 The Society of Photo-Optical Instrumentation Engineers; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; (12 pages).

Dale Ferriere and Khrystyna Pysareva and Andrezej Rucinski; Using Technology to Bridge Maritime Security Gaps; Aug. 1, 2005; Sea Technology; pp. 1-6; copyright Compass Publications, Inc. Jan. 2009; Portsmouth, New Hampshire, USA; (6 pages).

Corie Lok; Cargo Security; MIT Technology Review; Jun. 2004; No. 107; pp. 74-75; publisher is Massachusetts Institute of Technology; Cambridge, Massachusetts, USA; (2 pages).

Thomas C Chen; RFID and Sensor-based Container Content Visbility and Seaport Monitoring system; Proceedings of SPIE, vol. 5778; pp. 151-159; Mar. 28, 2005; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; (10 pages).

United States Department of Homeland Security; The University of Texas at Austin College of Engineering Standard Resume of Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-21; (21 pages).

* cited by examiner

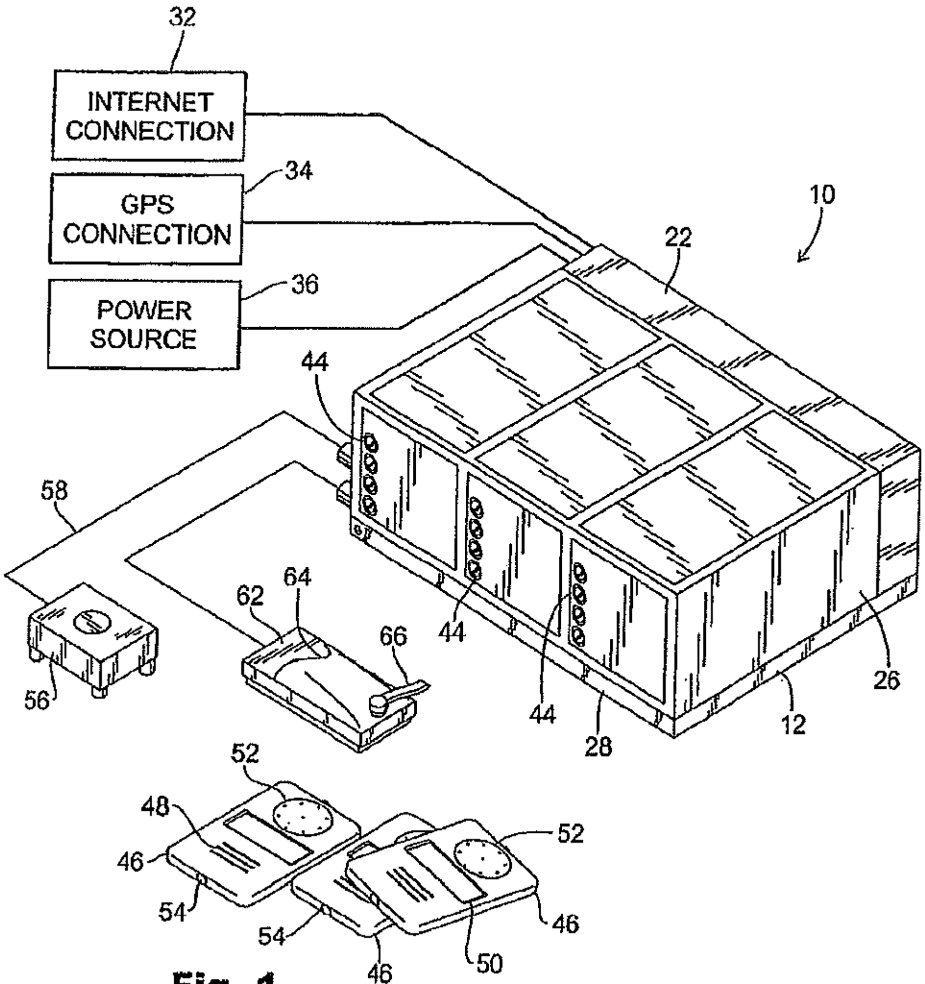

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
44
58
44
44
26
62
64
66
56
44
28
12
52
48
52
46
54
54
46
46
50

Fig. 1

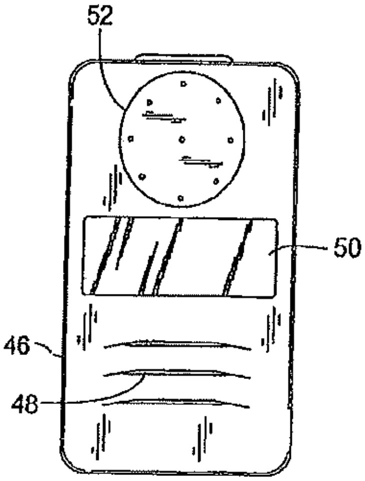

52
50
46
48

Fig. 2

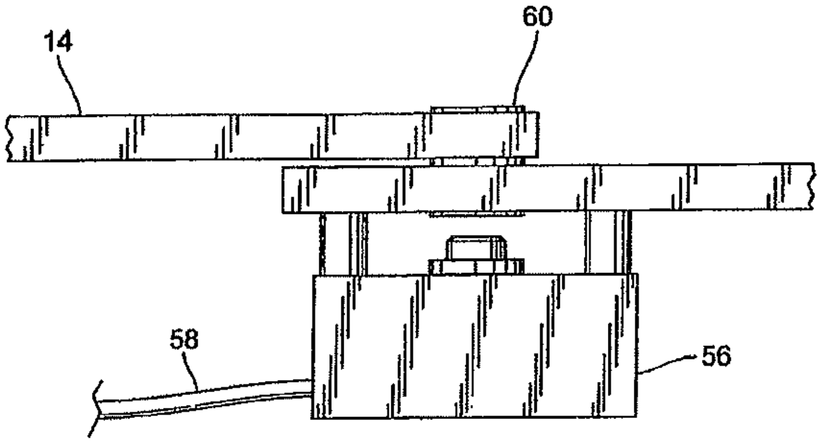


Fig. 3a

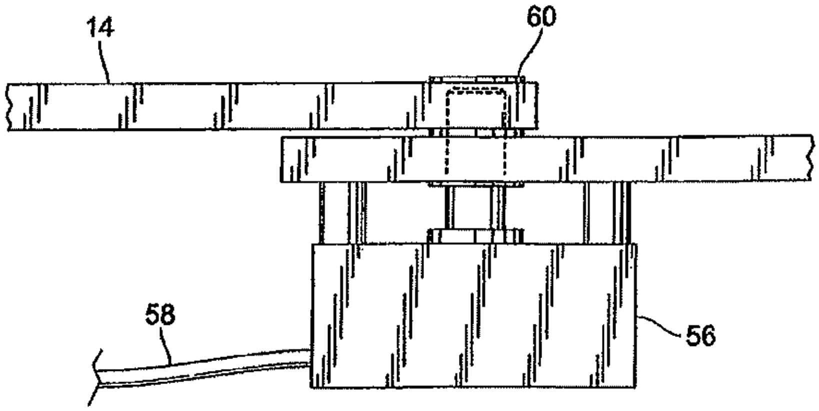


Fig. 3b

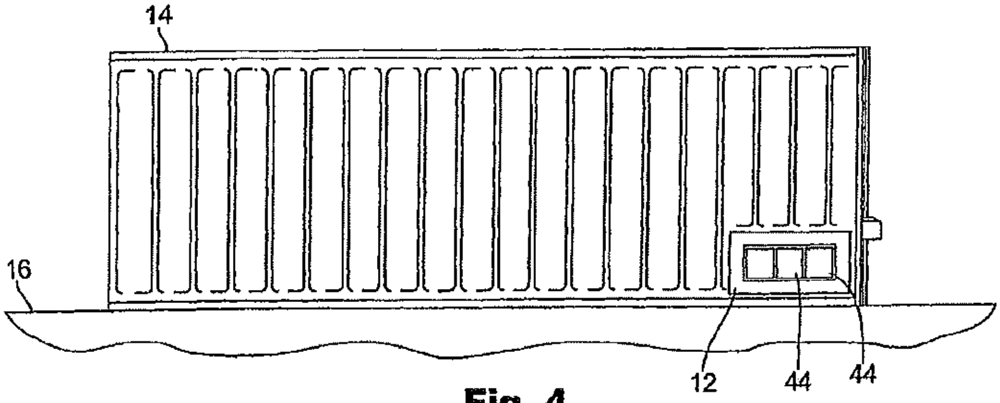


Fig. 4

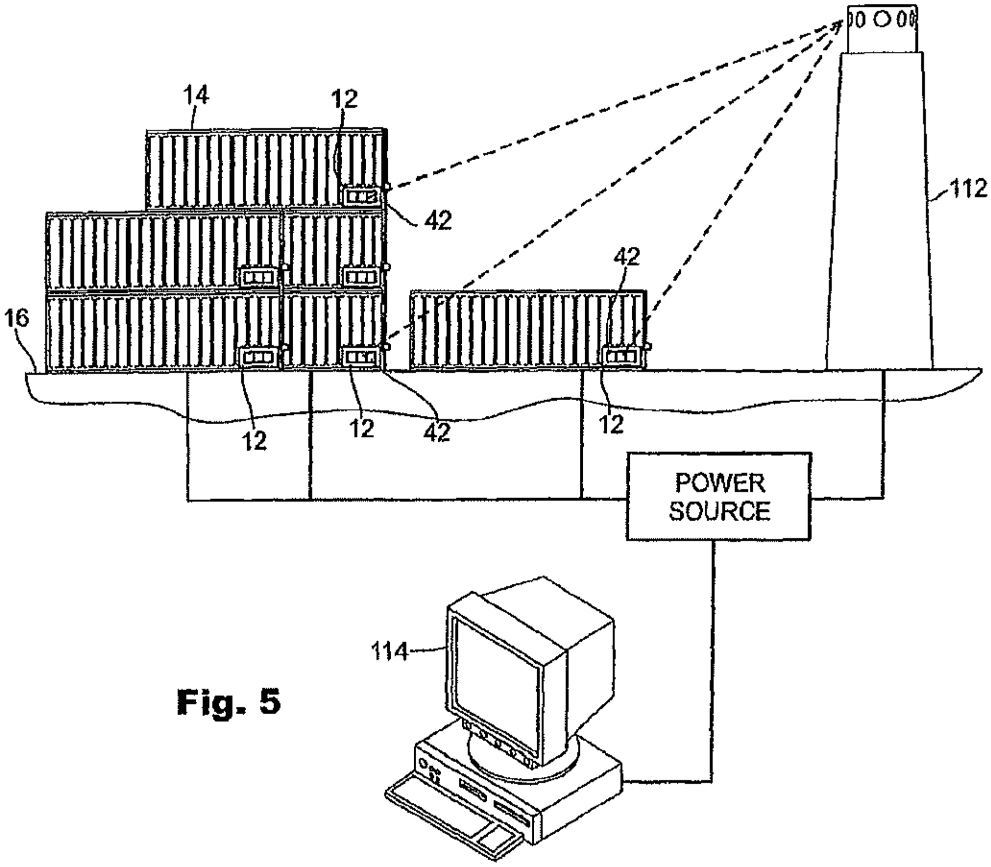


Fig. 5

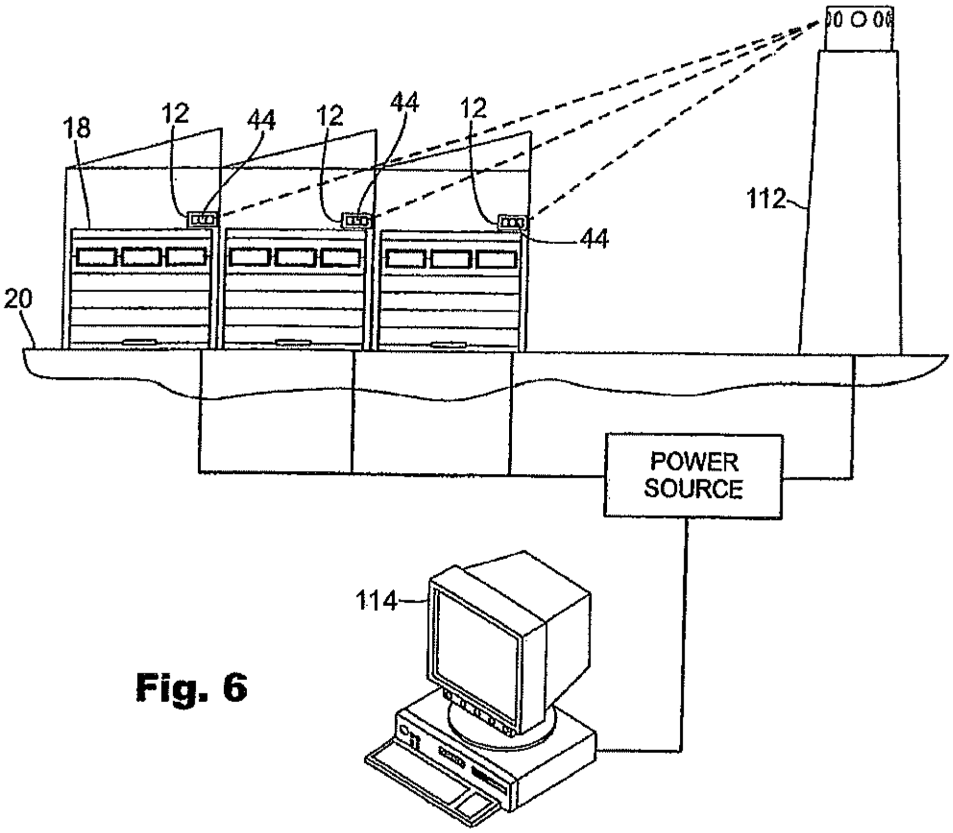


Fig. 6

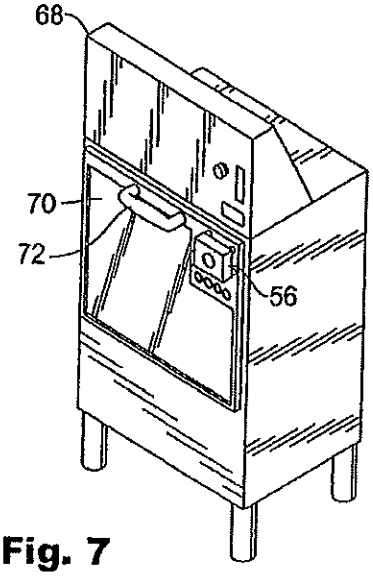


Fig. 7

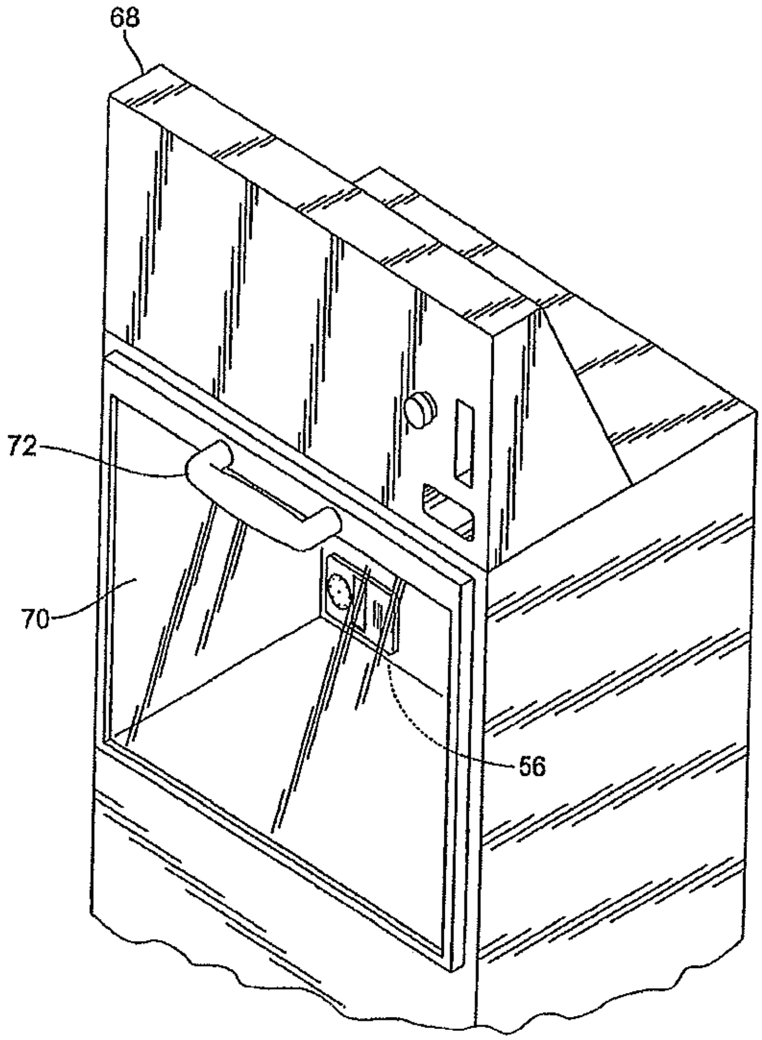


Fig. 8

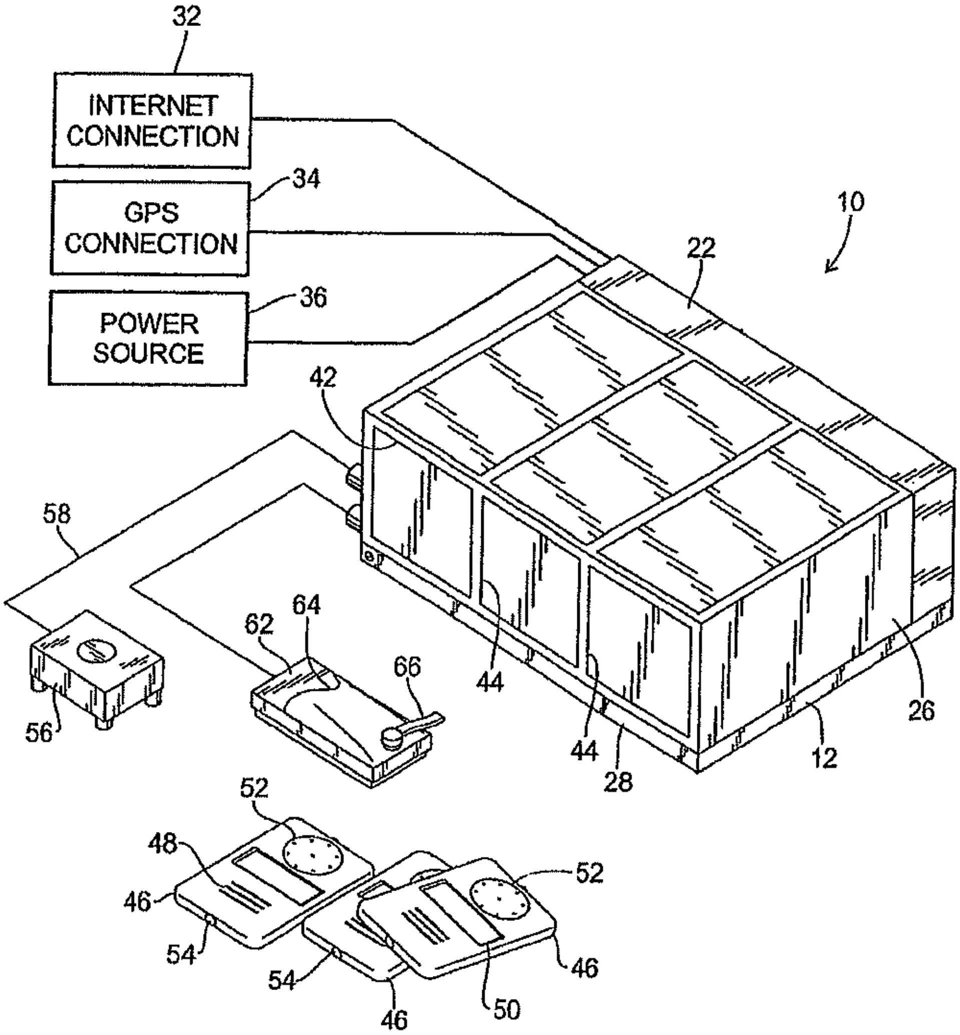

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
42
58
62
64
66
44
44
26
12
28
56
52
48
46
54
54
46
50
52
46

Fig. 9

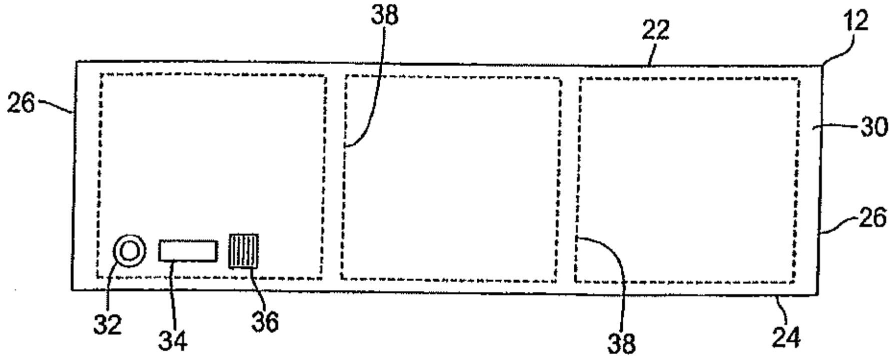

38
22
12
26
30
26
32
34
36
38
24

Fig. 10

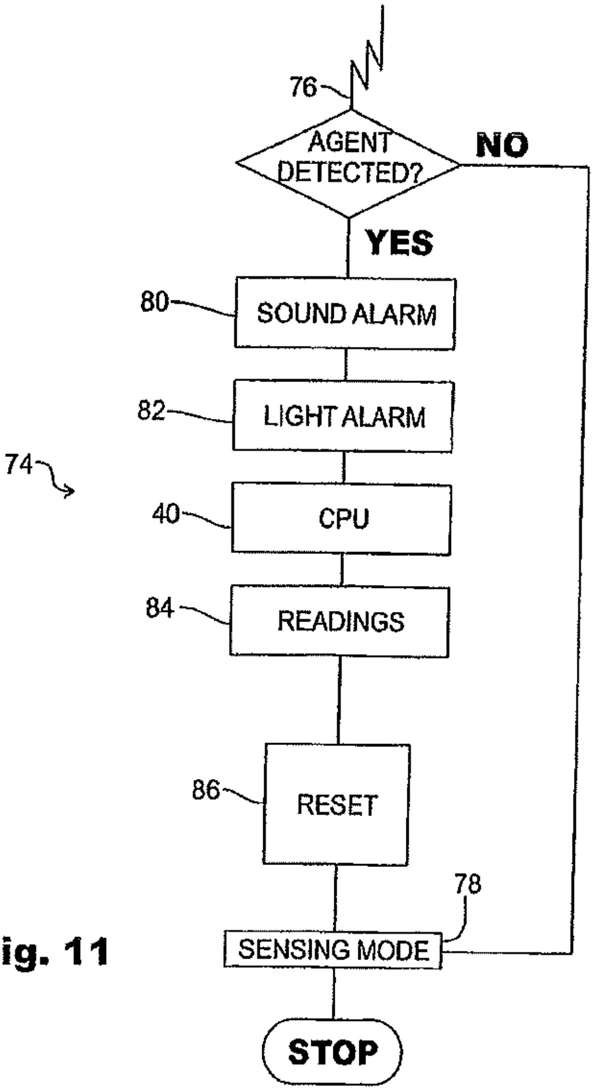

76
AGENT DETECTED?
NO
YES
80
SOUND ALARM
82
LIGHT ALARM
74
40
CPU
84
READINGS
86
RESET
78
SENSING MODE
STOP

Fig. 11

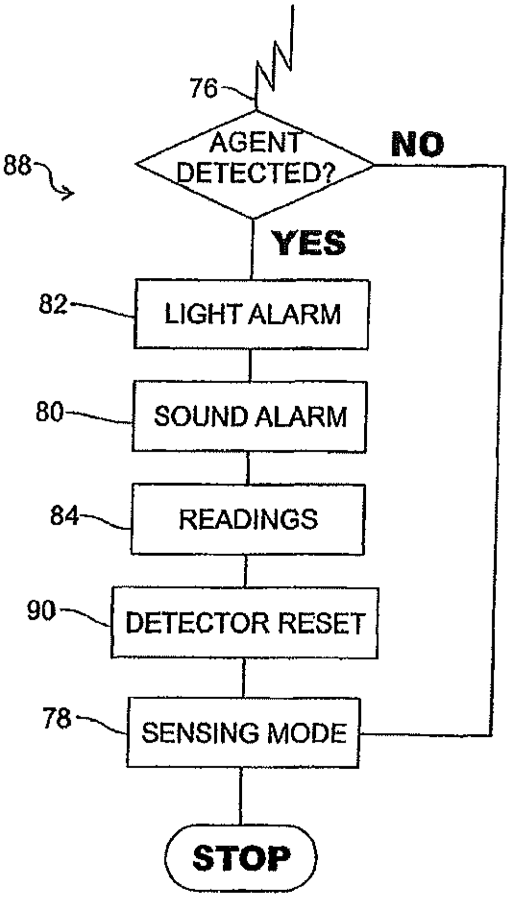

76
88
AGENT DETECTED?
NO
YES
82
LIGHT ALARM
80
SOUND ALARM
84
READINGS
90
DETECTOR RESET
78
SENSING MODE
STOP

Fig. 12

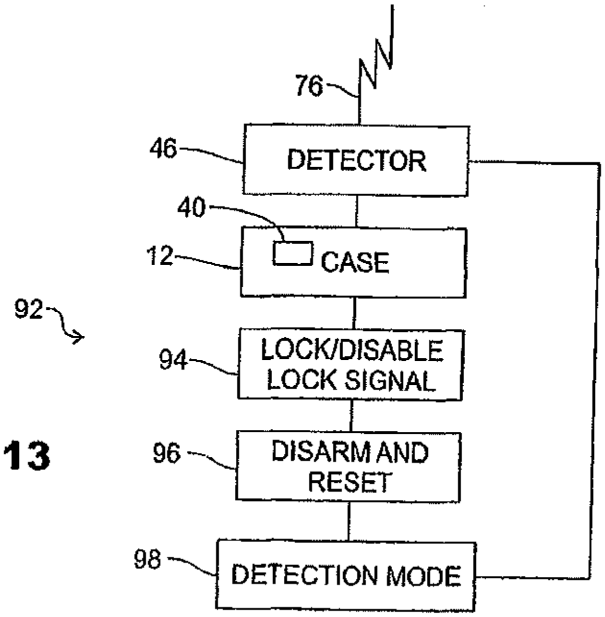

76
46
DETECTOR
40
12
CASE
92
94
LOCK/DISABLE LOCK SIGNAL
96
DISARM AND RESET
98
DETECTION MODE

Fig. 13

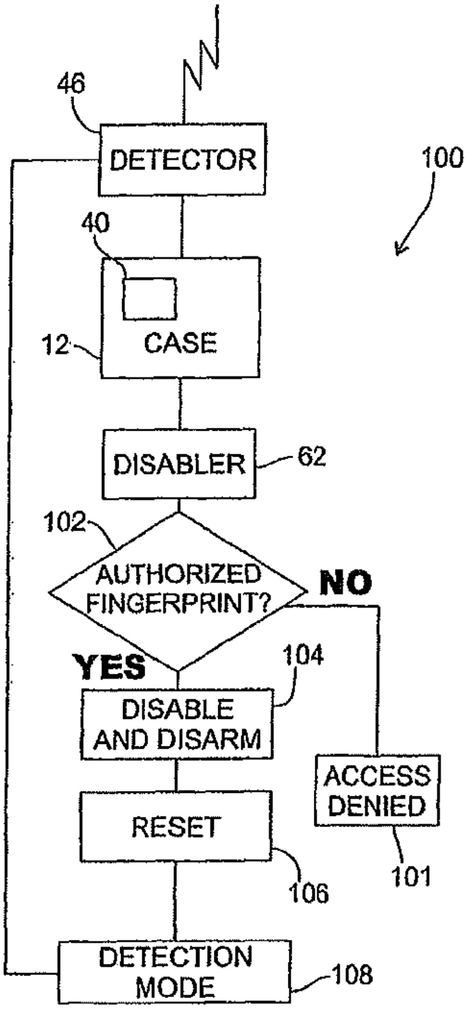

46
DETECTOR
100
40
12
CASE
DISABLER
62
102
AUTHORIZED FINGERPRINT?
NO
YES
104
DISABLE AND DISARM
ACCESS DENIED
RESET
101
106
DETECTION MODE
108

Fig. 14

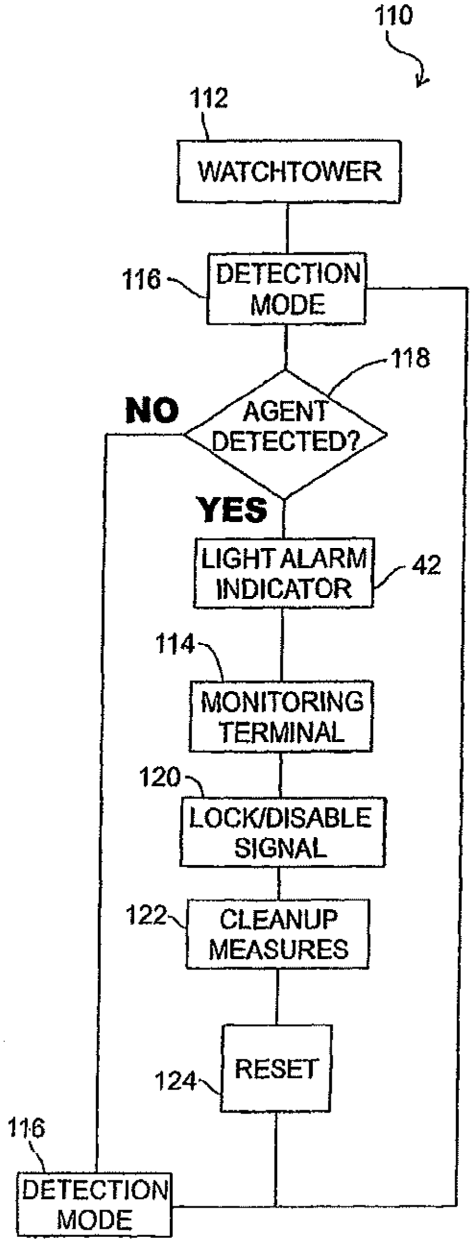

110
112
WATCHTOWER
116
DETECTION MODE
118
NO
AGENT DETECTED?
YES
LIGHT ALARM INDICATOR
42
114
MONITORING TERMINAL
120
LOCK/DISABLE SIGNAL
122
CLEANUP MEASURES
124
RESET
116
DETECTION MODE

Fig. 15

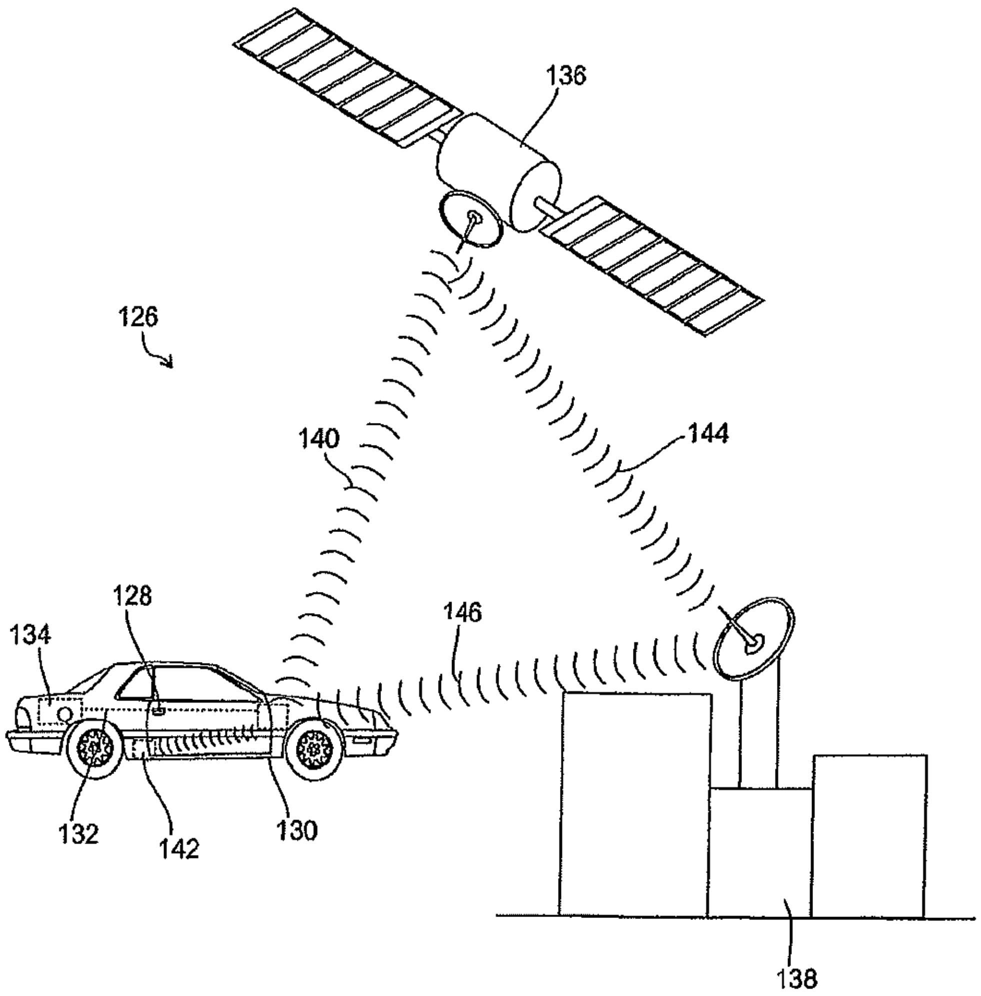


Fig. 16

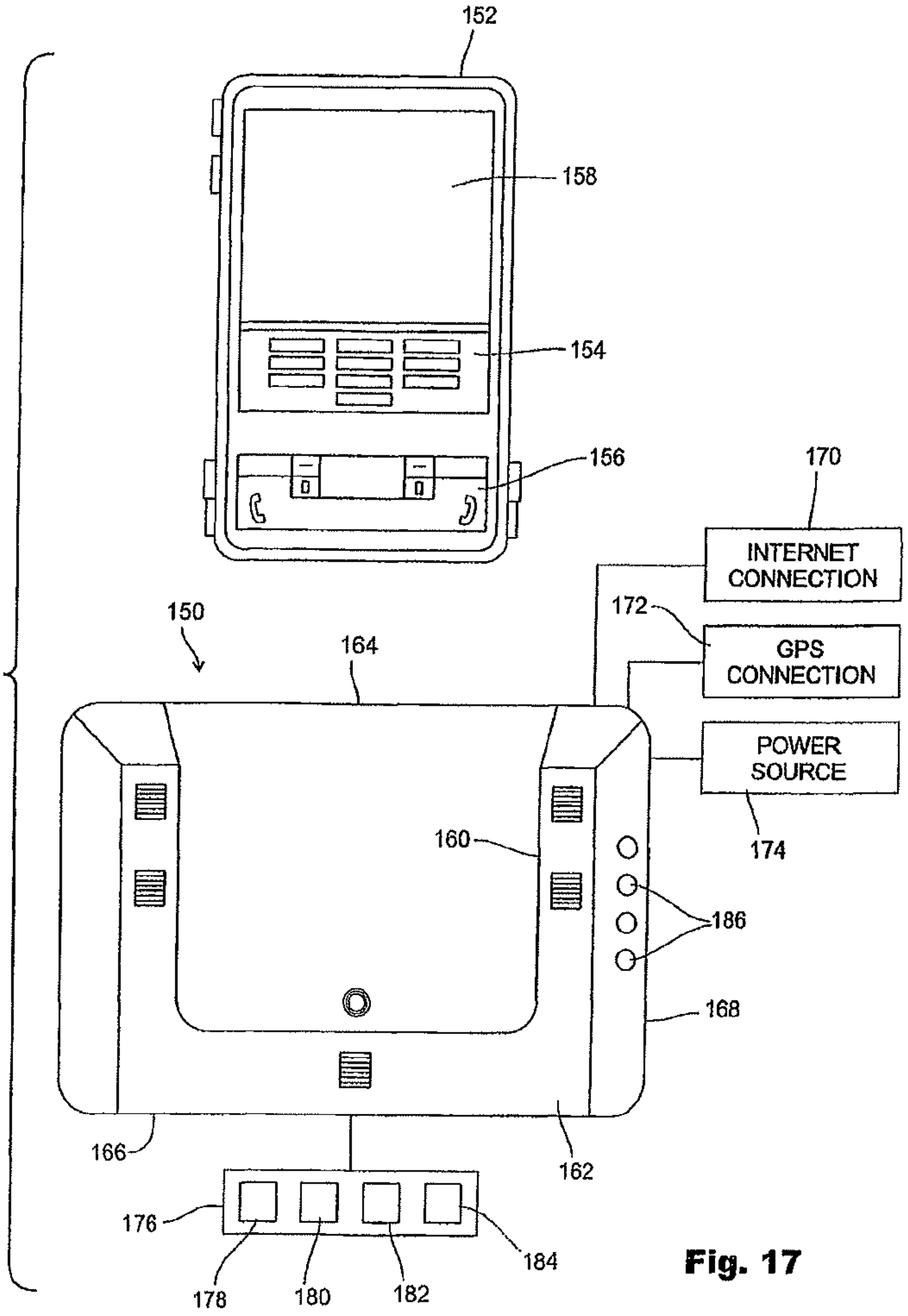

152
158
154
156
170
INTERNET CONNECTION
172
GPS CONNECTION
POWER SOURCE
174
150
164
160
186
168
166
162
176
184
178
180
182

Fig. 17

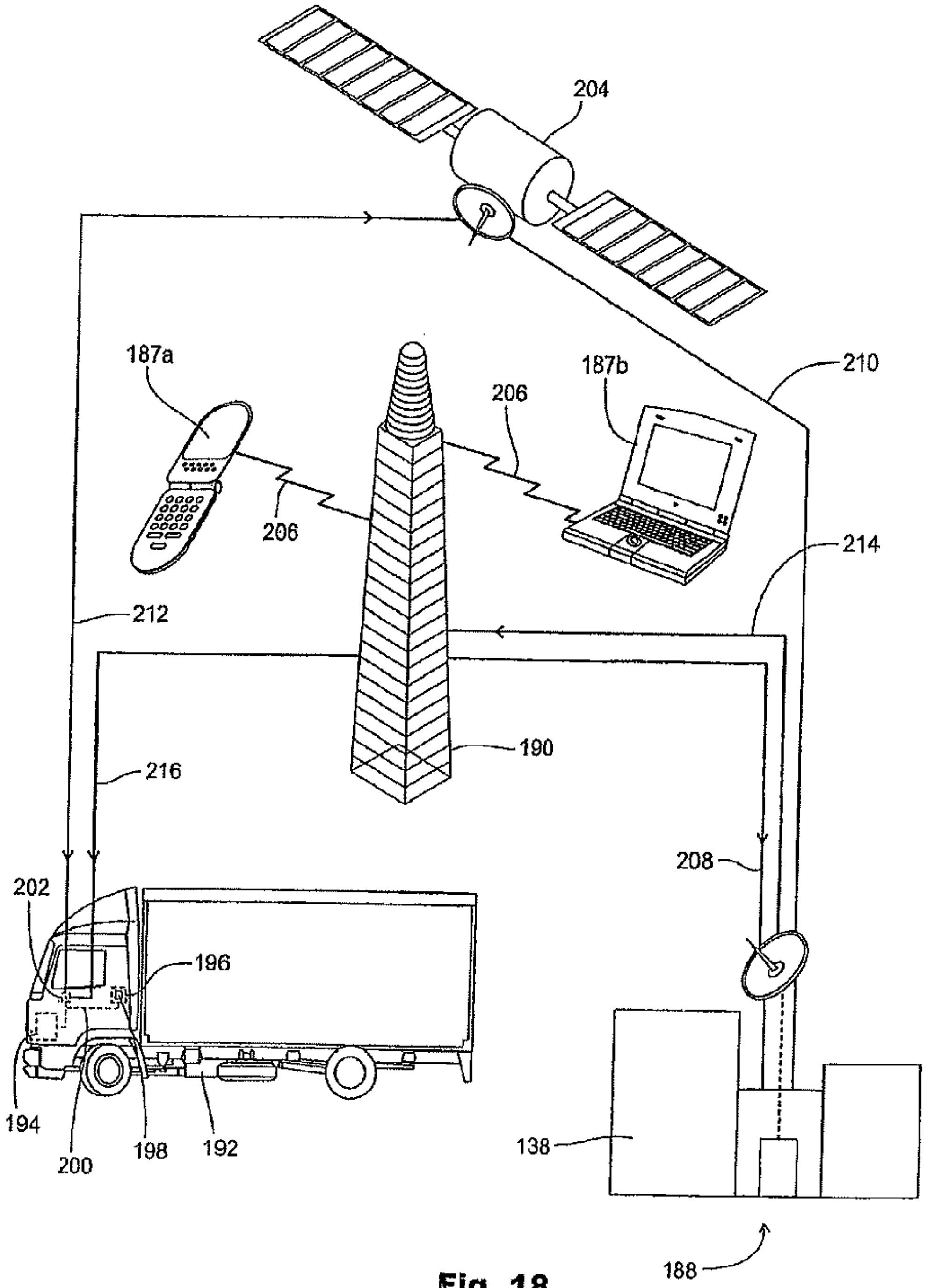

204
187a
206
187b
210
206
214
212
216
190
208
202
196
194
200
198
192
138
188

Fig. 18

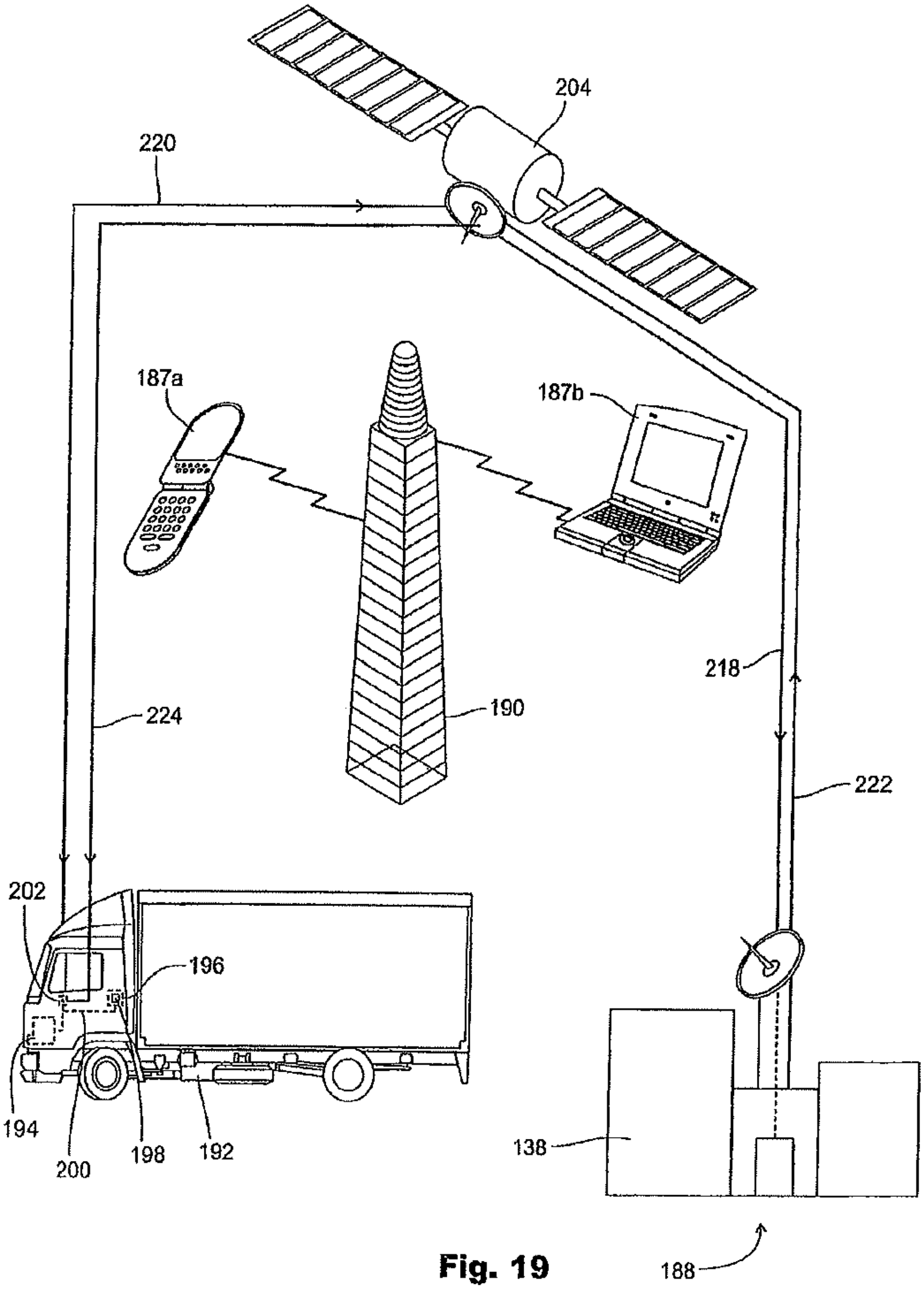

204
220
187a
187b
218
224
190
222
202
196
194
200
198
192
138
188

Fig. 19

MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM

This application is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 13/288,065 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Nov. 3, 2011 and that will issue on Sep. 10, 2013 as U.S. Pat. No. 8,531,280, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 13/288,065 that will issue as U.S. Pat. No. 8,531,280 is a divisional application and claims the filing date and benefit of U.S. patent application Ser. No. 12/802,001 titled "Multi Sensor Detection, Stall to Stop, and Lock Disabling System" filed on May 27, 2010, now U.S. Pat. No. 8,334,761, the entire contents and complete subject matter of which is are incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 12/802,001 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 12/657,356 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Jan. 20, 2010, now U.S. Pat. No. 8,106,752 and incorporates the entire contents and complete subject matter therein by reference in their entirety for all purposes. U.S. patent application Ser. No. 13/288,065 that will issues as U.S. Pat. No. 8,531,280 also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/657,356, now U.S. Pat. No. 8,106,752 herein by reference for all purposes. The present application also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/802,001, now U.S. Pat. No. 8,334,761 by reference herein for all purposes. The present application also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/657,356, now U.S. Pat. No. 8,106,752 herein by reference for all purposes.

FIELD OF THE INVENTION

The present invention pertains to anti-terrorist detection and prevention systems, and more particularly pertains to a disabling lock mechanism combined with a chemical/biological/radiological detection system for use with products grouped together by similar characteristics in order to prevent unauthorized entry, contamination and terrorist activity.

BACKGROUND OF THE INVENTION

Terrorist activity is a continuous, daily, worldwide threat to the stability, prosperity, security and peace within nations and between and among nations. Its danger lies in its arbitrary destructiveness as much as in its unpredictability, and the constant threat of terrorist activity compels measures and actions that cause strain and contention in free, democratic societies as security concerns and civil liberty concerns must be balanced so that both public safety and civil liberties are maintained. Safety and security concerns can be addressed through numerous proactive steps and measures, many of which cause only minimal interference with and disruption of the daily routines of work, travel, commerce and entertainment. However, because modern industrial societies afford almost limitless places, locations, and opportunities for terrorist activities, no safety measure or security protocol will be foolproof, but many security measures, systems and protocols can be implemented that greatly minimize specific threats through fingerprint identification procedures, chemical, biological, and radiological hazard detections, bomb and

explosive detection, and controlling the access to everything from shipping containers to school lockers. Thus, the prior art discloses a wide range of security measures and systems.

For example, the Fishbine et al. patent (U.S. Pat. No. 4,792,226) discloses an optical fingerprinting system that includes an optics/processor unit, a video monitor, a data terminal, and a printer for collecting and storing data characteristics of all ten individual fingerprints for printing demographic information and fingerprint images as desired on a standard booking or applicant card.

The Schiller patent (U.S. Pat. No. 4,544,267) discloses a finger identification unit that includes a fingerprint scanning apparatus using a collimated beam of light to interrogate the fingerprint of a finger placed against a platen so that successive scan positions produce signals containing fingerprint information.

The Fishbine et al. patent (U.S. Pat. No. 5,222,152) discloses a portable fingerprint scanning apparatus for optically scanning and recording fingerprint images and wirelessly transmitting such images to a mobile processing unit for verification and background checking.

The Lougheed et al. patent (U.S. Pat. No. 5,233,404) discloses an optical scanning apparatus that uses a linear charge coupled device (CCD) for recording the image of a fingerprint on the viewing surface.

The Groger et al. patent (U.S. Pat. No. 5,766,956) discloses a diode laser based sensor for undertaking optical, chemical, immunological or nucleic acid-based assay or other chemical analysis.

The Feldman patent (U.S. Pat. No. 5,938,706) discloses a multi element security system for preventing the unauthorized use of an automotive vehicle, and which includes numerous locking and control features interconnected to an onboard cpu.

The Bowker et al. patent (U.S. Pat. No. 5,963,657) discloses a safety access control for doors, handles, locks, etc., wherein the surface relief of a finger is read and verified to either allow or prevent access by the individual to the door, handle, lock, etc.

The Bonder et al. patent (U.S. Pat. No. 6,078,265) discloses a fingerprint identification security system wherein a key lock operated security system utilizes the fingerprint of the individual to control user access to the security system, such as the ignition system of an automotive vehicle.

The Anzai et al. patent (U.S. Pat. No. 6,271,745 B1) discloses a keyless authorization system for use of a motor vehicle that includes fingerprint reading units located on the exterior or interior of the motor vehicle and which is coupled to a control unit for scanning, comparing and matching fingerprints to allow or disallow access to the motor vehicle.

The Hwang patent (U.S. Pat. No. 6,374,652 B1) discloses a fingerprint-activated doorknob in which a detecting sensor for a fingerprint is placed on the doorknob for measuring and searching the fingerprint against previously stored fingerprint inputs to control access to the door.

The Vor Keller et al. patent (U.S. Pat. No. 6,588,635 B2) discloses a safety holster for a firearm that includes a pivotally mounted retaining member and a fingerprint sensor for scanning fingerprint information so that only authorized users can withdraw the firearm from the holster.

The Cordery et al. patent (U.S. Pat. No. 6,613,571 B2) discloses a method and system for detecting biological and chemical hazards in the mail that includes sensors placed within the mail box for sampling and testing ambient air and so that mail can be safely transported through the mail system.

The Nagata patent (U.S. Pat. No. 6,628,213 B2) discloses a coding method for digital signal coding and decoding that includes a CMI (code-marked inversion) method of signal coding.

Nonetheless, despite the ingenuity of the above devices, methods, and systems, there remains a need for a multi-detector and disabling lock system for use with various types of products collected together by common characteristics into product groupings for detecting chemical, biological and radiological agents and compounds and for selectively disabling and activating the product locks thereby preventing unauthorized entry and further contamination and preventing and thwarting terrorist activities.

SUMMARY OF THE INVENTION

The present invention comprehends a chemical/biological/radiological detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes and lockers; while the products grouped into what may be referred to as Product grouping 2 include, but are not limited to, chemical, biological, radiological, and nuclear detectors, motion sensors and door sensors. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The multi sensor detection and lock disabling system includes a detector case sized to fit in, upon or adjacent any of the aforedescribed products for detecting harmful and dangerous chemical, biological, and radiological agents, compounds and elements. In addition, the multi sensor detection and lock disabling system is capable of transmitting a signal to lock or disable a lock on the product, and is also capable of transmitting signals to a monitoring computer terminal or PC so that appropriate defensive and safeguarding actions can be undertaken and an authorized individual can disarm and reset the locking system and the multi sensor detection system. The detector case includes a power source (battery or electrical), interior compartments, Internet and GPS connections and a cpu interconnected with the Internet and GPS connections, and also interconnected with one or more off site monitoring computer terminals or PCs. The detector case includes one or more light alarm indicators that are externally visible and that light up when the chemical, biological, or radiological agent or compound is detected, and the light alarm indicators (which can be indicator lights or panels on the front of the detector case) can be color coded for denoting the specific agent or compound detected, i.e., separate and distinct colors for indicating detection of the chemical, biological, or radiological agent or compound.

The detector case is designed to hold within the interior compartments one or more interchangeable detectors, and each detector is adapted and set up to sample a specific compound or agent. Each detector includes a sound alarm, a sensor, a light alarm, and a readings panel, and is electrically interconnected (either by wire or wirelessly) to the cpu of the detector case so that information regarding the detection of the particular agent or compound can be conveyed from the detectors to the detector case cpu. Each detector can also be used as a manual, stand-alone hand held scanner.

The multi sensor detection and lock disabling system can be interconnected to a surveillance watchtower, as well as monitoring computer terminals or PCs, with the watchtower scanning shipping and cargo crates and containers being prepared for shipment or sitting for extended periods of time on a dock or at a port, at a railway site, or at an industrial storage facility. The watchtower will scan the cargo and shipping crates and containers for the light alarm indicators on detector cases that are mounted in or upon the crates and containers, and thus continuous security surveillance of the crates and containers can be maintained.

An enhanced version of the multi sensor detection and lock disabling system can be employed to prevent car and vehicle bombings. Coupling the multi sensor detection and lock disabling system with satellite service will enable the detection system to detect explosives and transmit an alert signal by satellite to monitoring equipment at a monitoring site. Upon receiving the alert signal at the monitoring site the monitoring equipment activates a stall-to-stop process for disabling the air, fuel, electrical and/or computer system of the vehicle. Moreover, upon receiving the alert signal at the monitoring site the car or vehicle will be locked by transmission of a satellite signal that disables the vehicle's electrical and ignition system thereby preventing escape of the terrorist.

It is an objective of the present invention to provide a multi sensor detection and disabling lock system for securing news racks and vending machines in order to prevent theft, unauthorized use and terrorist activity.

It is another objective of the present invention to provide a multi sensor detection and disabling lock system for preventing terrorist activity by using products grouped together by common features in several product groupings such as design similarity, similarity in the presentation of security problems and similarity with regard to the presentation of solutions to preventing terrorist solutions.

It is still yet another objective of the present invention to provide a multi sensor detection and disabling lock system that is capable of disabling an existing lock or activating a lock inside any of the products of the product grouping lists when a detector or sensor of the system is activated.

It is still yet a further objective of the present invention to provide a multi sensor detection and disabling lock system wherein the disabling lock system prevents the unauthorized entry, access and further contamination of the products included in the several product groupings.

A still further objective of the present invention is to provide a multi sensor detection and lock disabling system that utilizes a multi-task device for preventing terrorist activity to vulnerable products that are collected or arranged by product grouping categories.

Yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system to secure cargos and containers, especially cargo and shipping containers, against chemical, biological, radiological and nuclear terrorist activity.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system capable of detecting chemical, biological and radiological agents and compounds.

Still yet another objective of the present invention is to provide a multi sensor detection and disabling lock system that includes interchangeable detectors that operate in conjunction to detect chemical, biological and radiological agents and compounds.

Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories.

Another objective of the present invention is to provide a multi sensor detection and disabling lock system that accurately and reliably detects harmful agents, compounds and elements, and prevents the placement and storage of weapons and bombs in the range of storage containers and facilities currently available.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system wherein the interchangeable detectors that comprise part of the system can be used as stand-alone scanners.

These and other objects, features, and advantages will become apparent to those skilled in the art upon a perusal of the following detailed description read in conjunction with the accompanying drawing figures and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the primary features of the system which include a detector case, several interchangeable detectors, an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler;

FIG. **2** is a front elevation view of the multi sensor detection and lock disabling system of the present invention illustrating one of the interchangeable detectors first shown in FIG. **1**;

FIG. **3***a* is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one lock disabler to the lock of a product, such as a container, and disengaged from the lock of the container;

FIG. **3***b* is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the engagement of the lock disabler to the lock of the product for locking or disabling the lock of the product so that unauthorized access is prevented;

FIG. **4** is a side elevation view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case mounted to the product, such as the container, with the light alarm indicators externally visible;

FIG. **5** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of detector cases with a surveillance watchtower and a monitoring PC terminal;

FIG. **6** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the placement of detector cases upon containers different from the containers of FIG. **5**, and wherein the detectors case are interconnected to a surveillance watchtower and a monitoring PC terminal;

FIG. **7** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one automatic/mechanical lock disabler to the lock of a standalone news rack;

FIG. **8** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating one interchangeable detector placed within the standalone news rack;

FIG. **9** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case having color coded front panels for specifically indicating the agents, compounds or elements that have been detected;

FIG. **10** is a rear elevation view of the multi sensor detection and lock disabling system of the present invention illustrating the GPS, Internet and power source connections;

FIG. **11** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector with the detector case and the steps undertaken by the system when an agent or compound is detected;

FIG. **12** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the sequence of steps undertaken by one detector when functioning as a standalone scanner for detecting an agent or compound;

FIG. **13** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector case with the automatic/mechanical lock disabler for activating the lock disabler upon detection by the system of an agent or compound;

FIG. **14** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating interconnection of the detector case with the fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public upon detection of the agent or compound;

FIG. **15** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the system with a surveillance watchtower and a monitoring PC or computer terminal for monitoring containers, such as shipping or cargo containers, that may sit for extended time periods on docks, at rail yards, and at industrial storage facilities;

FIG. **16** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the integration of the detection system with a satellite and monitoring equipment at a monitoring site for detecting explosives placed in a vehicle and then transmitting signals to the satellite and then to the monitoring site for disabling and locking the vehicle;

FIG. **17** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the features and elements of the detector case to a cell phone and cell phone case;

FIG. **18** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of a GPS satellite, a monitoring site and a cell phone tower for communicating to and with an electronic device such as a laptop computer or a cell phone for transmitting signals to a vehicle for activating an onboard stall-to-stop device for bringing the vehicle to a halt; and

FIG. **19** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the use of a GPS satellite in conjunction with the monitoring site and monitoring equipment to relay commands and signals to the cpu or transceiver of the vehicle for stopping or locking the vehicle in response to a signal that a certain type of event (detection of a bomb, engine failure or malfunction or unauthorized use) has occurred or is in process

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Illustrated in FIGS. **1-19** is a multi sensor detection and lock disabling system **10** for preventing terrorist activity by monitoring, detecting, and securing those critical areas, sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities that are vulnerable to terrorist activity as convenient places to store and plant explosives and bombs and spread biological, chemical or radiological agents and compounds, followed by the disposition of the multi sensor detection and lock disabling system **10** for monitoring, detecting, and securing the particular location or site. Vulnerable sites, locations, facilities and areas are nearly limitless in their variety; in order to categorize the protection the present invention provides an anti-terrorist product grouping strategy has been developed wherein products made from the same or similar material, products having the same or similar design, and products presenting the same or similar security problems are grouped together with the multi sensor detection and lock disabling system **10** for preventing terrorist activity. For example, two preferred product groupings can be Product Grouping I: cargo containers, shipping containers, cargo planes, freight train cars, tractor trailers, mail carriers (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans and utility vehicles. Product Grouping II: chemical detectors, biological detectors, radiological detectors, nuclear detectors, motion sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems. In addition to grouping products together by features, designs and materials, the multi sensor detection system **10** includes a lock disabling capability for disabling an existing lock or activating a lock on or inside any of the aforementioned products when a detector or sensor of the system is activated. The lock disabling feature is a crucial component of the invention in so far as it prevents unauthorized, unequipped or untrained individuals from gaining access and entry to the site and causing further contamination of the site.

As shown in FIGS. **1-10**, the multi sensor detection and lock disabling system **10** includes at least one—and preferably many—detector case **12** that can be placed in, on, upon or adjacent the product, such as the shipping containers **14** of FIGS. **4** and **5** resting upon a platform **16** or the cargo container **18** of FIG. **6** sitting upon a seaport dock or pier **20**. The detector case **12** includes a top **22**, a bottom **24**, a pair of opposed sides **26** and a front side or panel **28** and an opposite rear or back side **30**. The rear side **30** has connections or contacts that can include an Internet connection **32**, a GPS connection **34** and a power connection **36** for a power source. The power source for the detector system **10** can be any conventional battery or electrical source. The detector case **12** includes an interior chamber divided into a number of compartments **38** for holding therein agent or compound detection means hereinafter further described. A cpu **40** is mounted within the detector case **12** and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment. The front side **28** of the detector case **12** includes indicator means for visually indicating that a specific agent, compound or element has been detected. The indicator means can include color coded indicator lights **42** in panel form, as shown in FIG. **9**, with each indicator light panel **42** lighting up with a specific color corresponding to the detection of a specific agent or compound; or color coded indicator lights **44**, as shown FIG. **1**, that correspond to and individually light up on the detection of a specific agent or compound (chemical, biological, or radiological).

As shown in FIGS. **1**, **2** and **9-13**, the multi sensor detection and lock disabling system **10** includes a plurality of detectors **46** with each detector **46** adapted for and set up to sample for a specific agent or compound (biological, chemical, or radiological); and the detectors **46** are interchangeable for adapting to the needs and demands of future technology. The detectors **46** can also be used as standalone scanners. In the preferred embodiment of the invention, at least three detectors **46** are placed within the detector case **12** with one detector **46** for specifically sampling biological agents or compounds, one detector **46** for sampling chemical agents or compounds, and one detector **46** for sampling radiological agents or compounds. The detectors **46** are interconnected to the cpu **40** of the detection system **10** by conventional connections that can be wire or wireless for transmitting the appropriate signals to the cpu **40** upon detection of the particular agent or compound. As shown in FIG. **2**, each detector **46** includes on its front plate or facing surface a sound alarm indicator **48**, a readings panel **50** comprising a plastic shield and LED lights for displaying the various read-out messages, a sensor **52** for detecting the specific agent, element or compound, and a light alarm indicator **54** that can be color coded for each specific agent and which is externally visible when the detector **46** is used as a stand alone scanner. Each detector **46** includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the cpu **40** of the detector case **12**.

As shown in FIGS. **1**, **3***a*, **3***b*, **9**, and **13-15**, used in conjunction with the multi sensor detection and lock disabling system **10** is at least one automatic/mechanical lock disabler **56**—and depending upon the number of products being monitored there can be one lock disabler **56** for each product. The automatic/mechanical lock disabler **56** is physically connected to the detector case **12** by a wire or cable **58** for receiving signals therefrom for disabling an existing lock or activating a lock inside a product to prevent access to the product. By way of example, FIG. **3***a* shows the automatic/mechanical lock disabler **56** mounted—by any conventional means—to the lock **60** of the shipping container **14** shown in FIGS. **4** and **5** and connected by wire **58** to the cpu **40** of the detector case **12**. The lock disabler **56** is in the non-activated or disengaged state in FIG. **3***a*. FIG. **3***b* shows the automatic/mechanical lock disabler **56** mounted to the lock **60** of the shipping container **14** and in the activated or engaged state after detection of an agent or compound by the system **10** thereby for locking or disabling the lock **60** of the shipping container **14** and preventing unauthorized entry and access by unauthorized, untrained and unequipped individuals. In FIGS. **3***a* and **3***b* the lock **60** secures doors of the shipping container **14** that can be slidably or pivotably opened and closed.

In addition to the automatic/mechanical lock disabler **56**, the multi sensor detection and lock disabling system **10** can also utilize a fingerprint biometric lock with disabler **62** as shown in FIGS. **1** and **14**. The fingerprint biometric lock with disabler **62** is interconnected to the cpu **40** of the detector case **12** for receiving transmissions therefrom after detection of an agent or compound has occurred so that the lock on the product can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler **62** occurs when the fingerprint of the individual is placed on the fingerprint-matching pad **64**, and if a match occurs with a known fingerprint stored by the cpu **40**, then the individual can reset the fingerprint biometric lock with disabler **56** by turning the manual lock disabler **66**. The fingerprint biometric lock with disabler **62** is mounted to the lock of the product in a manner similar to the mounting of the automatic/mechanical lock disabler **56** that is shown in FIGS. **3** and **3***b*.

FIGS. **4** and **5** show one manner of disposition or placement of the detector case **12** in relation to the product, i.e., the shipping container **14**, with the color coded indicator lights **42** externally viewable; FIG. **5** shows a number of shipping containers **14** each equipped with a detector case **12** and integrated with elements hereinafter further described for continuously monitoring the shipping containers **14** as they sit for an extended period of time on the truck or rail platform **16**. FIG. **6** illustrates several cargo containers **18** sitting on the shipping dock or pier **20**, with each cargo container **18** having a detector case **12** mounted thereon and integrated with and monitored by elements shown in FIG. **5** and hereinafter further described.

FIG. **7** illustrates a typical product from product grouping 1 that is monitored by the multi sensor detection and lock disabling system **10** of the present invention; specifically, FIG. **7** shows a news rack **68** with one automatic/mechanical lock disabler **56** mounted to and interconnected with the locking mechanism of the news rack **68**. As long as there is no detection of any agent or compound, the lock disabler **56** is in the disengaged state, and the individual can deposit the coin amount in the chute and then freely open the glass panel **70** by the handle **72** for removing a paper. However, the lock disabler **56** would be activated upon detection of the harmful agent or compound and receipt of a signal from the cpu **40** for locking or disabling the locking mechanism thereby denying access to the interior of the news rack **68** from all untrained, unauthorized and unequipped individuals.

FIG. **8** illustrates one detector **46** disposed within the news rack **68** and which is visible through the panel **70** for detecting one specific agent, compound or element. The detector **46** functions as a stand-alone scanner and can be wirelessly interconnected to offsite monitoring equipment.

FIG. **11** illustrates a representative schematic **74** for describing the signal transmission process from the detector **46** to the cpu **40** of the detector case **12**. The external stimulus **76** would be the chemical, biological or radiological agent or compound. If there is no detection of the agent or compound, the detector **46** will stay in the sensing mode **78**. However, detection of the specific agent will trigger the sound alarm **80** and the light alarm **82**, and instant transmittal of a signal to the cpu **40**. The readings **84** can be stored by the cpu **40** for verification and future review and evaluation. After all the appropriate corrective and preventative measures have been undertaken by the trained and authorized personal, and the site has been cleansed of the contamination, authorized and equipped personal can then reset **86** the system **10**.

FIG. **12** illustrates a representative schematic **88** for the detector **46** when used as stand-alone scanner. The detector **46** undergoes the same essential steps as illustrated in FIG. **11**, with the exception of the signal transmission to the cpu **40**. The detector **46** remains in detection mode **78** until an agent is detected, and then the various functions—light alarm **82**, sound alarm **80**, storage of readings **84**, and, after the appropriate security and safety steps have been carried out by authorized personal, detector reset **90** by authorized personal can occur thereby placing the detector **46** back in detection or sensing mode **78**.

FIG. **13** is a representative schematic **92** that illustrates the steps undertaken by the system **10** to lock or disable a lock, such as the lock **60** for the shipping container **14** shown in FIGS. **3***a* and **3***b*. Upon detection of the agent (chemical, biological, radiological) the alarm light indicators **42** or **44** will light up providing external indication that an agent has been detected. In addition, the system **10**—the cpu **40**—will transmit a lock/disable lock signal **94** to the automatic/mechanical lock disabler **56** to lock or disable the lock on the product, such as the lock **60** on the shipping container **14** of FIGS. **3***a*-**5**. This prevents unauthorized, unequipped, or untrained individuals from entering or gaining access to the product for which a dangerous and perhaps lethal agent has been detected. After the proper authorities and authorized personal have been notified and all the appropriate security, preventative and clean up measures have been undertaken, the authorized individual can perform the disarm and reset function **96** for the system **10** placing the system **10** in back in the detection mode **98**.

FIG. **14** is a representative schematic **100** illustrating the use of the fingerprint biometric lock with disabler **62** with the system **10**. Upon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the cpu **40** would then transmit a signal to the fingerprint biometric lock with disabler **62** to lock or disable the lock on the product, such as the lock **60** on the shipping containers **14** shown in FIGS. **3***a*-**5**. The shipping containers **60** would remain locked and in an access denied mode **101** should an attempt be made to gain access to the container **60** by opening the lock **60** with an unauthorized fingerprint. However, a fingerprint that matches stored and authorized fingerprints **102** would indicate an authorized individual, and would allow the individual to disable and disarm **104** the lock **60** of the shipping container **14**. The fingerprint biometric lock with disabler **62** would then be reset **106** after the appropriate safety, cleanup, and protection measures are completed, and the system **10** would be reset and placed back in the detection mode **108**.

FIG. **15** is a schematic representation **110** that illustrates the integration of a surveillance watchtower **112** and a monitoring terminal or PC **114** for monitoring products such as the shipping containers **14** or cargo containers **16** that sit for extended periods of time of docks, piers **20**, truck terminals, mil yards, shipping platforms **16** and industrial sites as shown in FIGS. **5** and **6**. The watchtower **112** would maintain continuous surveillance over a number of shipping containers **60**, for example, with detector cases **12** mounted in or on each container **14** and set in detection mode **116** with one or more detectors **46** disposed in each detector case **12**. The watchtower **112** would continuously scan for light alarm indicators **42** and **44** on the products, such as the containers **14** or **18**, and the watchtower **112** would be interconnected and integrated with the monitoring terminal or PC **114**. Upon detection **118** of an agent or compound in one or more of the shipping containers **14**, the appropriate light alarm indicators **42** or **44** would light providing visible confirmation of the detection of the specific agent or compound. The cpu **40** would transmit a lock/disable signal **120** to the lock **60** on each respective shipping container **14** to lock or disable the lock **60** thus preventing access to that respective shipping container **14**. In addition, signal transmissions would be sent to the monitoring terminal or PC **114** (which could be off site) thereby alerting authorized security personal of the contamination event. With the information received at the monitoring terminal **114**, authorized personal would then be notified and dispatched to the area to undertake the appropriate safety and cleanup measures **122**. Such measures would also include disarming the lock disabling system in order to gain access to the shipping container **14**. After all the cleanup and security measures are completed by the trained and properly equipped authorities, the detection system and the lock disabling feature would reset **124** and the detection system would again be placed in detection mode **116**.

FIG. **16** is a schematic representation **126** that illustrates an enhanced version of the multi sensor detection and lock disabling system **10** for preventing car and vehicle attacks and bombings. The lock disabling system **10** would be interconnected to the locking system and mechanism **128** of the vehicle **130**. In addition, a stall to stop disabling link **132** can be made with the fuel, air, and electrical system **134** of the vehicle **130**. The enhanced version incorporates a satellite **136** for signal receipt and transmission from the vehicle **130** in which the detector system **10** is placed to a monitoring site and monitoring equipment **138**. As shown in FIG. **16**, a detection signal **140** would be sent to the satellite **136** by the detection system **10** upon detection of a bomb or explosive **142** hidden in the vehicle **130**. The satellite **136** would then transmit an alert signal **144** to the monitoring site **138** with the signal **144** containing the relevant data to evaluate the nature of the threat. The monitoring site **138** would then transmit a stall to stop signal **146** to the detection system **10** to lock the vehicle **130** and/or disable the electrical system of the vehicle **130** thereby disabling the vehicle **130**, preventing access to the vehicle **130** by locking the vehicle **130**, and preventing any terrorist in the vehicle **130** from escaping.

The detector case **12** can be modified and adapted for inclusion with cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, and briefcases. In addition, the basic monitoring terminal or PC **114**, as shown in FIGS. **5** and **15**, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring.

The system **10** and the watchtower **112**, along with the satellite **136** and the monitoring site **138** can be adapted or incorporated with cell phone towers and satellites for use with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu **40**, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween. The aforementioned telecommunication and radio communication means can be interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships and airplanes, and which is reported stolen, experiences a loss of brakes, or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted to the vehicle and which detection causes an automatic signal transmission or a signal transmission is activated when a call is made to the monitoring station by an authorized person. The authorized individual includes but is not limited to the owner, pilot, conductor, captain, police highway patrol, security guard and military personnel to the monitoring equipment for activating a vehicle slowdown or stall-to-stop disabling system that similar to the disabling system **126** shown in FIG. **16**, or incorporating features of the system **126** shown in FIG. **16**, from the monitoring equipment to the vehicle. The activation of the stall-to-stop disabling means or the vehicle slowdown disables or engages the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.

In addition, the basic stall-to-stop disabling means or the vehicle slowdown means and device can be adapted, modified or designed to include: an open bust or open platform for integrating any new and innovative technology; warning lights indicators; sound alarm indicators; voice alarm indicators; a cell phone to transmit to the vehicle a signal for slowing and halting the vehicle; and a lock disabling system or means to lock a thief or terrorist inside the vehicle after a transmission is received or sent. Open bust or open platform also refers to the compatibility of the detector case **12**, or the incorporation of its features in cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, briefcases, and suitcases, etc., with other communication, transmission and surveillance systems whereupon the detector case **12**, and its features, can be seamlessly integrated with other new and emerging systems and technologies.

Thus, as shown more specifically in FIG. **17**, by way of a representative example the features and elements of the detector case **12** are shown as being incorporated into cell phone detector case **150** and associated cell phone monitor **152**. The cell phone monitor **152** includes the standard keypad functions **154** and more specialized system use (ring tone, email, photos, texting) functions **156** as well as a viewing screen **158**. The cell phone detector case **150** includes a recharging cradle or seat **160**, a front side **162**, a top **164**, a bottom **166**, and a pair of opposed sides **168**. At the back of the cell phone detector case **150** are connections, contacts, and ports for at least an Internet connection **170**, a GPS connection **172**, and a contact, plug, or port for a power source **174**. The power source for the cell phone detector case **150** can be any conventional rechargeable battery source or standard electrical power from a standard electrical receptacle or outlet.

As shown in FIG. **17**, the cell phone detector case **150** includes one or more sensor/detector units, cells, or components **176** built into and incorporated into the case **150**. The detector **176** includes generally disposed at the front **162** of the case **150** the following types of indicators: a sound alarm indicator **178**, a readings panel **180**, a sensor **182** for detecting one or more specific types of agents, elements, chemicals, compounds, etc., and a light alarm indicator **184**. The sensor/detector **176** will be interconnected to the power source **174**. In addition, mounted on and externally visible on the sides **168** or front **162** of the case **150** are a plurality of color coded indicator lights **186** with each light **186** corresponding to a specific agent, element, chemical, compound, etc., and lighting up when that agent is detected by the sensor/detector **176**. The color coded indicator lights **186** will be electrically interconnected to the sensor/detectors **176** via any standard microprocessor. The cell phone detector case **150** and cell phone monitor **152** thus comprise a hand-held, easily portable and transportable detection means that is both effective and unobtrusive in its disposition and use.

FIGS. **18** and **19** illustrate representative examples of the integration of portable electronic communication or telecommunication devices such as a cell phone **187***a* and/or a laptop computer **187***b* with the monitoring equipment **138** located at a predesignated monitoring site **188**, and operating in conjunction with either a satellite and/or a cell phone tower **190** to transmit and receive signals and commands among each other and to a vehicle **192**, such as a truck, as part of a stall-to-stop disabling system for slowing and stopping the vehicle **192** and locking a thief, terrorist, or unauthorized individual in the vehicle **192** if needed. A wide range of events can trigger and initiate the stall-to-stop system and the locking or lock disabling system and mechanism, and the event doesn't have to be limited to the detection of a bomb or a chemical, biological, or radiological agent, element, or compound. The events can include, but is not limited to, detection of an engine problem to engine failure to the unauthorized use (stealing) of the vehicle **192**. The vehicle **192** includes an electromotive system **194** that comprises, among other components, an onboard computer(s), electrical, fuel and air systems, as well as brakes, ignition, steering, and transmission. Also integrated with and capable of communicating with the vehicle's **192** electromotive system **194** is a stall-to-stop system while a lock disabling mechanism **196** is able to engage and disengage or disable the vehicle's **192** locking mechanism **198** upon receipt of the appropriate commands via a lock disabling communication channel or link **200**. This link **200** can also accommodate the stall-to-stop system commands and signals, and thus is a multi-channel communication link. A CPU or a transceiver **202** is programmed to receive signals from the cell phone tower **190** and/or to a GPS satellite **204** and is interconnected with the stall-to-stop system and the lock disabling system **196** via link **200** for engaging the electromotive system **194** and actuating the lock disabling system **196** to stop the vehicle **192** and lock inside the vehicle **192** anyone such as a thief, terrorist or other unauthorized individual.

A representative example for stopping, disabling, and locking the vehicle **192** that utilizes the cell phone tower **190** wherein the activation and/or distress signal **206** originates from the cell phone **187***a* or the laptop **187***b* and such activation signal **206** travels to the cell phone tower **190** that is nearest the current location of the vehicle **192**. A signal **208** is then transmitted to the monitoring site **188** and specific monitoring equipment **138** that can also include but is not limited to cell phones, laptops, desktop PC's, notebook PC's and LCD monitors. The monitoring site **138** then communicates by signal **210** to the GPS satellite **204** that an original or activation signal has been received and then the GPS satellite **204** locates and communicates by multiplex signal **212** with the CPU or transceiver **202** on the vehicle **192** and exchanges information on the type of problem, situation, location, and vehicle speed. The monitoring equipment **138** then transmits a signal **214** to the cell phone tower **190** that communicates with the transceiver **202** and/or CPU of the vehicle **192** to initiate or execute any commands that will actuate the stall-to-stop disabling link **200** and lock disabling system **196** for bringing the vehicle **192** to a halt and actuating the vehicle's **192** locking mechanism **198** for locking the thief, terrorist, or other unauthorized person inside the vehicle **192** if needed.

FIG. **19** illustrates a representative example wherein the stall-to-stop system and the lock disabling system **196** are utilized in conjunction with the GPS satellite **204**. In FIG. **19** a signal has traveled to the satellites nearest the vehicle's **192** current location and then the signal **218** has traveled to the monitoring equipment **138** and monitoring site **188** which can include but is not limited to satellite cell phones, satellite monitors, cell phones, laptops, desktop PC's, notebook PC's, and LCD monitors. The OPS satellite **204** then locates and communicates with the CPU and/or transceiver **202** on the vehicle **192** via a multiplex (two-way) signal **220** in order to exchange information on such distress and danger event parameters as the specific problem situation, location, and vehicle speed. The monitoring equipment **138** then transmits a signal **222** back to the GPS satellite **204** that in turn communicates via another signal **224** with the CPU and/or transceiver **202** to execute any commands to the stall-to-stop system for executing the disengagement of the vehicle's **192** electromotive system **194** for bringing the vehicle **192** to a halt and for actuating the lock disabling system **196** to direct the lock disabling link **200** to actuate the locking mechanism **198** thereby locking the vehicle **192** and anyone inside the vehicle **192**.

While the invention has been shown and described in a preferred embodiment, it will be apparent to those skilled in the art that numerous alterations, modifications, and variations will possible and practicable without departing from the spirit and scope of the invention as set forth by the appended claims.

The present invention comprehends a chemical/biological/radiological/nuclear/explosive/human/contraband detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars, (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans, UAVs, UGVs, and utility vehicles; the products grouped into what may be referred to as Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, door sensors, speed sensors, biometric sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems, detection of humans, detection of contraband, temperature, and shock levels; the products grouped into what may be referred to as Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, eyeglass, briefcases, detector cases of locks, detector cases of tags, detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to; the products grouped into what may be referred to as Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, web servers, desktop PCs, notebook PCs, laptops, satellite cell phones, cell phones, UMTS phones, PDAs, LCD monitors, and satellite monitoring, remote control key fobs, two-way communication key fobs, handhelds; the products grouped into what may be referred to as Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), General Packet Radio Services (GPRS), Global System for Mobile (GSM), Wideband Code Division Multiple Access (W-CDMA), Universal Mobile Telecommunications System (UMTS), Short Message Service (SMS); the products grouped into what may be referred to as Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature. the products grouped into what may be referred to as Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, HAZMAT, CIA, FBI, Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside or outside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The invention claimed is:

1. A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:

at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;

a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;

at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;

the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;

wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;

wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;

wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).

2. Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:

at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;

a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;

a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;

at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;

monitoring equipment of at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the monitoring equipment, is interconnected to a product equipped to receive signals from or send signals to the lock disabling mechanism that is able to engage and disengage or disable the lock, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;

wherein the monitoring equipment is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products.

3. Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:

at least one of a central processing unit (CPU), a network processor, or a microprocessor for executing and carrying out the instructions of a computer program or application which is specifically targeted at the networking application domain, for communication between the monitoring equipment and any of a plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device;

a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device;

a receiver for receiving signals, data or messages from at least one of plurality of product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device, wherein the signals, data or messages are of agents of an item of interest (IOI);

at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or GPS connection;

the monitoring equipment is at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the monitoring equipment, is capable of the activation or deactivation of at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device;

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, for signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of a chemical agent, a biological agent, a radiological agent, a nuclear agent, or an explosive agent which allows radio frequency (RF) data to be received and transferred between the tag and the monitoring equipment.

4. A built-in, embedded multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents;

comprising a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;

comprising a communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a built-in sensor array or fixed detection device for communication therebetween,

wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;

wherein the built-in embedded multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories; and

wherein, when an alarm occurs, the built-in, embedded multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-long or short range radio frequency, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for communication therebetween;

wherein the built-in embedded multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity.

5. A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:

a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;

wherein the built-in multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);

wherein the built-in multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;

a light alarm indicator that has a plurality of colored lights that correspond to specific ones of the at least two agent;

wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween.

6. A built-in multi sensor detection system for detecting at least two items selected from the group consisting of chemical agent, biological agent, radiological agent, explosive agent, human agent, contraband agent, motion, perimeter, temperature, tampering, theft, and breach, comprising:

a built-in sensor array or fixed detection device into a product that detects items by means of at least two sensors from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;

wherein the built-in, multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);

wherein, when an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween,

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of the chemical agent, the biological agent, the radiological agent, the explosive agent, the human agent, the contraband agent, the motion, the perimeter, the temperature, the tampering, the theft, and the breach which allows radio frequency (RF) data to be received and transferred between the tag and the monitoring equipment.

7. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;

monitoring equipment comprising at least one of plurality product groups based on the categories of a computer, laptop, notebook, PC, handheld, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;

whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;

wherein the monitoring equipment or multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products;

wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;

wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).

8. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween, wherein the monitoring equipment is equipped with a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (to make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom; or at least one satellite capable of transmitting signals to the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment; and whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;

wherein the multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;

wherein the multi sensor detection device for any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products.

9. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device, wherein at least one of the sensors is capable of detecting agents of an item of interest (IOI);

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;

at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;

whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or from a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;

wherein the multi sensor detection device for any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, or broadband connection, is in signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of the explosive agent, the nuclear agent, the contraband agent, the chemical agent, the biological agent, the human agent, or the radiological agent which allows radio frequency (RF) data to be received and transferred between the tag and the monitoring equipment.

* * * * *

Exhibit B

US009589439B2

(12) **United States Patent**
Golden

(10) **Patent No.: US 9,589,439 B2**
(45) **Date of Patent: *Mar. 7, 2017**

(54) **MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM**

(71) Applicant: **Larry Golden**, Mauldin, SC (US)

(72) Inventor: **Larry Golden**, Mauldin, SC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 81 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/806,988**

(22) Filed: **Jul. 23, 2015**

(65) **Prior Publication Data**

US 2016/0027273 A1 Jan. 28, 2016

Related U.S. Application Data

(60) Continuation of application No. 14/021,693, filed on Sep. 9, 2013, now Pat. No. 9,096,189, which is a

(Continued)

(51) **Int. Cl.**

B60R 25/102	(2013.01)
G08B 13/24	(2006.01)
B60R 25/01	(2013.01)
B60R 25/04	(2013.01)
G07C 9/00	(2006.01)

(Continued)

(52) **U.S. Cl.**

CPC ***G08B 13/2491*** (2013.01); ***B60R 25/018*** (2013.01); ***B60R 25/04*** (2013.01); ***B60R 25/102*** (2013.01); ***G07C 9/00912*** (2013.01); ***G08B 15/00*** (2013.01); ***G08B 21/12*** (2013.01);

(Continued)

(58) **Field of Classification Search**

CPC G08B 15/00; G08B 15/001; G08B 15/004; G08B 25/009; B60R 25/102; B60R 25/01; B60R 25/018; B60R 25/04; B60R 25/0405; B60R 25/0415; B60R 25/10

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,385,469	A	5/1983	Scheuerpflug
4,544,267	A	10/1985	Schiller

(Continued)

OTHER PUBLICATIONS

United States Department of Homeland Security; Petition for Inter Partes Review of U.S. Pat. No. Re. 43,990 Under 35 U.S.C. §312 and 37 C.F.R. §42.104; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-57; copy enclosed (57 pages)

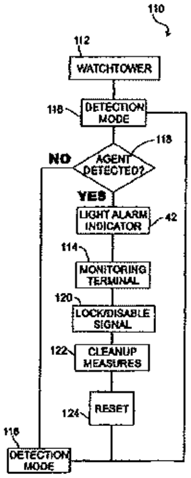
(Continued)

Primary Examiner — Van Trieu

(57) **ABSTRACT**

A multi sensor detection and disabling lock system includes detector cases for holding interchangeable detectors that sample for chemical, biological and radiological compounds, agents and elements, with each detector case disposed in or upon the monitored product. The detector case transmits detection information to a monitoring computer terminal and transmits a signal to a lock disabler engaged to the product to lock or disable the product's lock thereby preventing untrained, unauthorized and unequipped individual's from gaining access and entry to the product, and also preventing further contamination of the area. The detection system can be interconnected to surveillance towers scanning detector cases disposed at seaport docks, freight depots and rail terminals for monitoring containers being prepared for shipment or sitting on docks for long periods of time.

23 Claims, 13 Drawing Sheets



Related U.S. Application Data

continuation of application No. 13/288,065, filed on Nov. 3, 2011, now Pat. No. 8,531,280, which is a division of application No. 12/802,001, filed on May 27, 2010, now Pat. No. 8,334,761, which is a continuation of application No. 12/657,356, filed on Jan. 20, 2010, now Pat. No. 8,106,752, which is a continuation of application No. 12/155,573, filed on Jun. 6, 2008, now Pat. No. 7,636,033, which is a continuation-in-part of application No. 11/397,118, filed on Apr. 5, 2006, now Pat. No. 7,385,497.

(51) **Int. Cl.**
G08B 15/00 (2006.01)
G08B 21/12 (2006.01)

(52) **U.S. Cl.**
CPC ... *B60R 2325/205* (2013.01); *B60R 2325/304* (2013.01); *G07C 2009/0092* (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,586,441	A	5/1986	Zekich
4,792,226	A	12/1988	Fishbine
5,222,152	A	6/1993	Fishbine
5,223,844	A	6/1993	Mansell et al.
5,233,404	A	8/1993	Lougheed
5,557,254	A	9/1996	Johnson
5,682,133	A	10/1997	Johnson
5,766,956	A	6/1998	Groger
5,938,706	A	8/1999	Feldman
5,959,529	A	9/1999	Kail, IV
5,963,657	A	10/1999	Bowker
5,986,543	A	11/1999	Johnson
5,990,785	A	11/1999	Suda
6,049,269	A	4/2000	Byrd
6,078,265	A	6/2000	Bonder
6,262,656	B1	7/2001	Byrd
6,271,745	B1	8/2001	Arizal
6,374,652	B1	4/2002	Hwang
6,411,887	B1	6/2002	Martens
6,470,260	B2	10/2002	Martens
6,542,076	B1	4/2003	Joao
6,542,077	B2	4/2003	Joao
6,588,635	B2	7/2003	Vor Keller
6,610,977	B2	8/2003	Megerie
6,613,571	B2	9/2003	Cordery
6,628,813	B2	9/2003	Scott
6,647,328	B2	11/2003	Walker
6,738,697	B2	5/2004	Breed
6,923,509	B1	8/2005	Barnett
6,980,092	B2	12/2005	Turnbull
6,988,026	B2	1/2006	Breed et al.
7,005,982	B1	2/2006	Frank
7,034,677	B2	4/2006	Steinthal et al.
7,034,683	B2	4/2006	Ghazarian
7,103,460	B1	9/2006	Breed
7,109,859	B2	9/2006	Peeters
7,116,798	B1	10/2006	Chawla
7,148,484	B2	12/2006	Craig et al.
7,164,117	B2	1/2007	Breed et al.
7,171,312	B2	1/2007	Steinthal et al.
7,243,945	B2	7/2007	Breed et al.
7,339,469	B2	3/2008	Braun
7,346,439	B2	3/2008	Bodin
7,385,497	B2	6/2008	Golden
7,397,363	B2	7/2008	Joao
7,636,033	B2	12/2009	Golden
7,647,180	B2	1/2010	Breed
7,844,505	B1	11/2010	Arneson et al.
7,868,912	B2	1/2011	Venetianer et al.
7,872,575	B2	1/2011	Tabe
7,880,767	B2	2/2011	Chinigo
7,961,094	B2	6/2011	Breed
8,274,377	B2	9/2012	Smith et al.
8,531,521	B2	9/2013	Romanowich
8,564,661	B2	10/2013	Lipton
2002/0145666	A1	10/2002	Scaman
2003/0063004	A1	4/2003	Anthony et al.
2003/0137426	A1	7/2003	Anthony et al.
2003/0206102	A1	11/2003	Joao
2004/0107028	A1	6/2004	Catalano
2004/0222092	A1	11/2004	Musho
2005/0195069	A1	9/2005	Dunand
2006/0164239	A1	7/2006	Loda
2006/0176169	A1	8/2006	Doolin et al.
2006/0181413	A1	8/2006	Mostov
2006/0250235	A1	11/2006	Astrin
2007/0171042	A1	7/2007	Metes et al.
2008/0045156	A1	2/2008	Sakhpara
2008/0122595	A1	5/2008	Yamamichi
2008/0234907	A1	9/2008	Labuhn
2010/0159983	A1	6/2010	Golden
2011/0178655	A1	7/2011	Golden

OTHER PUBLICATIONS

United States Department of Homeland Security; Declaration of Dr. Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-44; copy enclosed (44 pages).

Richard R Brooks and S.S. Iyengar; Multi-Sensor Fusion Fundamentals and Applications with Software; published 1998; Copyright Prentice Hall PTR; Upper Saddle River, New Jersey, USA; pp. 1-20; copy enclosed (20 pages).

Ramanarayanan Viswanathan and Pramod K Varshney; Distriubted Detection with Multiple Sensors: Part 1—Fundamentals; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-11; vol. 85; No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; pp. 1-11; copy enclosed (11 pages).

Blum; Distributed Detection with Multiple Sensors: Part II—Advanced Topics; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-16; vol. 85, No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; pp. 1-11; copy enclosed (16 pages).

Victor Lesser; Distributed Sensor Networks a Multiagent Perspective; 2003; pp. 1, 2, 5, 6, 22, 26, 27, 36, 275, 320; copyright 2003 Kluwer Academic Publishers; AH Dordrecht, The Netherlands; copy enclosed (10 pages).

Samuel Blackman and Robert Popoli; Design and Analysis of Modern Tracking Systems; 1999; pp. 1, 2, 6, 472; copyright 1999 Artech House; Norwood, Massachusetts, USA; copy enclosed (4 pages).

Jean-Francois Chamberland; Decentralized Detection in Sensor Networks; 2003; pp. 407-416; IEEE Transactions on Signal Processing; vol. 51, No. 2; Urbana, Illinois, USA; copy enclosed (10 pages).

Oleg Kachirski and Ratan Guha; Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks; pp. 1-8; Proceedings of the 36th Hawaii International Conference on System Sciences; copyright 2003; Orlando, Florida, USA; copy enclosed (8 pages).

Lawrence A Klein; Sensor and Data Fusion A Tool for Information Assessment and Decision Making; 2004; pp. 1-4, 6, 81, 87-89; copyright 2004 The Society of Photo-Optical Instrumentation Engineers; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; copy enclosed (12 pages).

Dale Ferriere and Khrystyna Pysareva and Andrzej Rucinski; Using Technology to Bridge Maritime Security Gaps; Aug. 1, 2005; Sea Technology; pp. 1-6; copyright Compass Publications, Inc. Jan. 2009; Portsmouth, New Hampshire, USA; copy enclosed (6 pages).

Corie Lok; Cargo Security; MIT Technology Review; Jun. 2004; No. 107; pp. 74-75; publisher is Massachusetts Institute of Technology; Cambridge, Massachusetts, USA; copy enclosed (2 pages).

Thomas C Chen; RFID and Sensor-based Container Content Visibility and Seaport Security Monitoring system; Proceedings of SPIE, vol. 5778; pp. 151-159; Mar. 28, 2005; Publisher is SPIE—

(56) References Cited

OTHER PUBLICATIONS

the International Society for Optical Engineering; Bellingham, Washington, USA; copy enclosed (10 pages).

United States Department of Homeland Security; The University of Texas at Austin College of Engineering Standard Resume of Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-21; copy enclosed (21 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 11/397,118; mailed Nov. 14, 2007; Alexandria, Virginia, USA; pp. 1-12; parent U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; mailed Apr. 9, 2009; Alexandria, Virginia, USA; pp. 1-7; parent U.S. Appl. No. 13/288,065 (7 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; mailed Jul. 30, 2009; Alexandria, Virginia, USA; pp. 1-9; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/155,573; mailed Oct. 28, 2009; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/657,356; mailed Jul. 12, 2010; Alexandria, Virginia, USA; pp. 1-14; parent U.S. Appl. No. 13/288,065 (14 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/657,356; mailed Mar. 10, 2011; Alexandria, Virginia, USA; pp. 1-4; parent U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 13/065,837; mailed Jul. 18, 2011; Alexandria, Virginia, USA, pp. 1-9; parent U.S. Appl. No. 13/288,065 (4 pages).

A newspaper article of Mr. Melvin Sullivan and his family that references the date, Mar. 6, 2001; parent U.S. Appl. No. 13/288,065.

A letter of response Mr. Sullivan received from Pfeiffer & Gantt, PA, dated Sep. 16, 2002; parent U.S. Appl. No. 13/288,065.

A "Certificate of Existance" Bright Idea Inventor, LLC. Nov. 6, 2002; parent U.S. Appl. No. 13/288,065.

Operating Agreement of Bright Idea Inventor, LLC received from Pfeiffer & Gantt, PA, dated Nov. 13, 2002; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Congressman from Maryland, Elijah E. Cummings, dated Dec. 16, 2002; parent U.S. Appl. No. 13/288,065.

A newspaper article of Mr. Melvin Sullivan and Mr. Larry Golden, dated, Feb. 27-Mar. 5, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated May 21, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Office of the Vice President, Dick Cheney, dated Jun. 3, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated Oct. 1, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Lindsey O. Graham, dated Oct. 21, 2003; parent U.S. Appl. No. 13/288,065.

A letter sent to the President of the United States George W Bush, the President's Cabinet, the United States Senate and the Congressional Black Caucus, dated May 23, 2005; parent U.S. Appl. No. 13/288,065.

On Nov. 17, 2005, an "Inventor's Official Record of Invention", was filed in my name (Golden) at "The Law Office of David P. Gaudio, P.C.; the Inventors Network."; parent U.S. Appl. No. 13/288,065.

On Aug. 23, 2005, the "Disclosure Document Registration"; parent U.S. Appl. No. 13/288,065.

On Apr. 5, 2006, the "Patent Application" was filed in my name (Golden) at the United Staets Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

On Jun. 6, 2008, the "Continuance-In-Part, (CIP) Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

On Jan. 20, 2010, a "Continuation Application" (U.S. Appl. No. 12/657,356) was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033;"Swear Back"; in accordance to Title 37—Code of Federal Regulations Patents, Trademarks, and Copyrights; Apr. 8, 2011; parent U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033; "Swearback—History of Work"; Apr. 8, 2011; parent U.S. Appl. No. 13/288,065.

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed Apr. 14, 2011; Alexandria, Virginia, USA; pp. 1-16; parent U.S. Appl. No. 13/288,065 (16 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed Oct. 20, 2011; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed May 27, 2011; Alexandria, Virginia, USA; pp. 1-14; parent U.S. Appl. No. 13/288,065 (14 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802 001; copyright and mailing date Dec. 12, 2011, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Dec. 2, 2011, pp. 1-27, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (27 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Nov. 1, 2011, pp. 1-18, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (18 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and mailing date Jan. 13, 2012, pp. 1-34, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (34 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and mailing date Mar. 26, 2012, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and mailing date Feb. 22, 2012, pp. 1-38, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (38 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Feb. 22, 2012, pp. 1-25, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (25 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Aug. 24, 2012, pp. 1-4, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Nov. 28, 2012, pp. 1-11, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (11 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Apr. 16, 2013, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and mailing date Apr. 20, 2015, pp. 1-20, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 14/021,693 (20 pages).

(56) **References Cited**

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and mailing date Jan. 20, 2015, pp. 1-17, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 14/021,693 (17 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and mailing date Sep. 5, 2015, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 14/021,693 (12 pages).

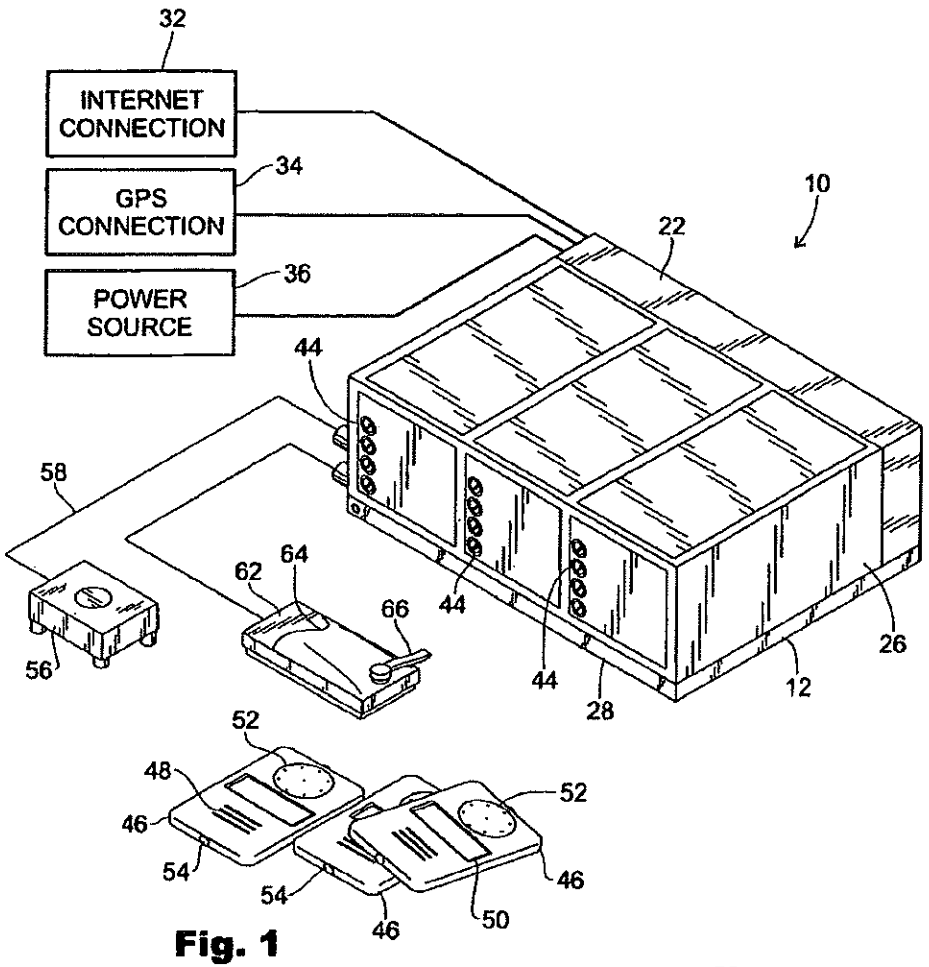

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
44
58
62
64
66
44
44
26
56
28
12
52
48
46
52
54
54
46
46
50

Fig. 1

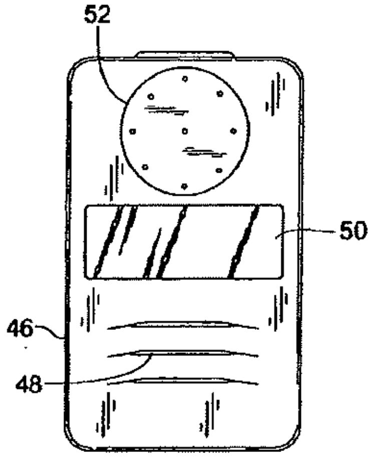

52
50
46
48

Fig. 2

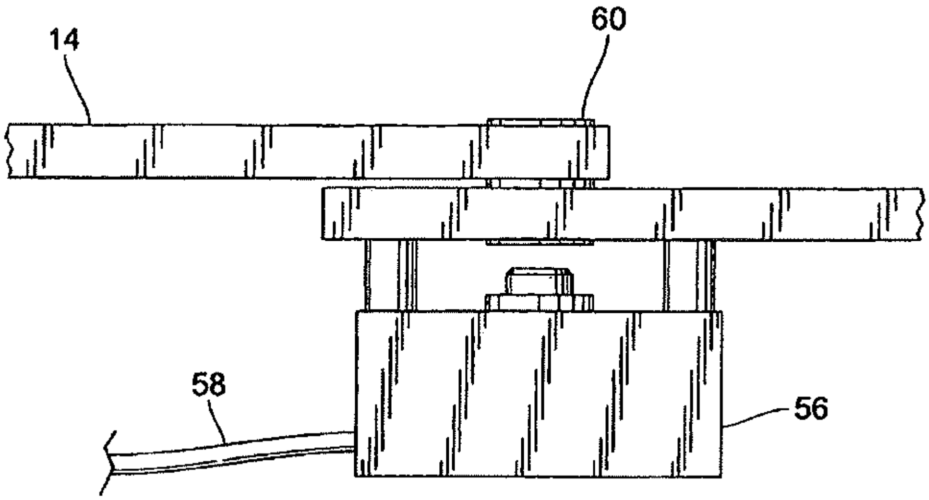


Fig. 3a

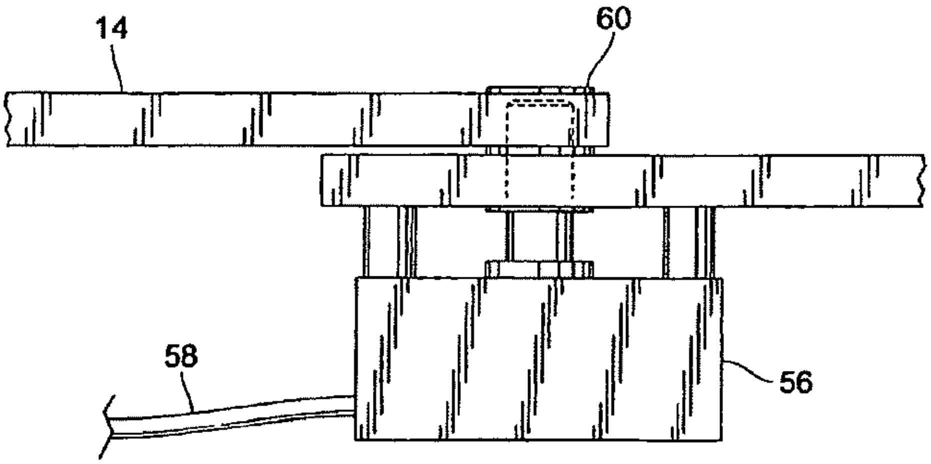


Fig. 3b

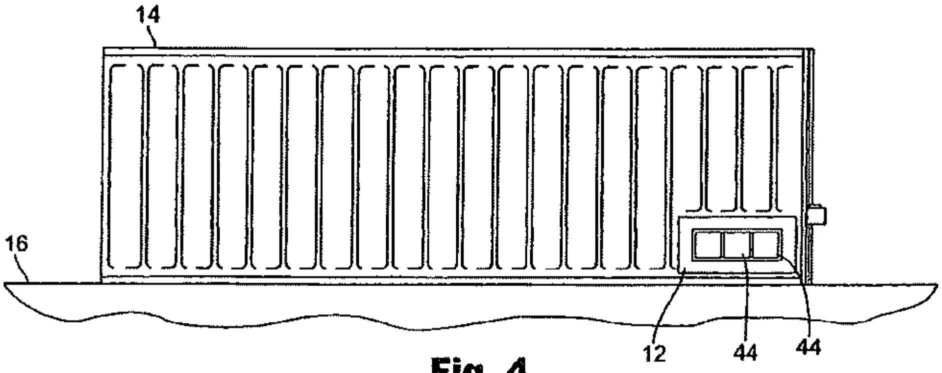


Fig. 4

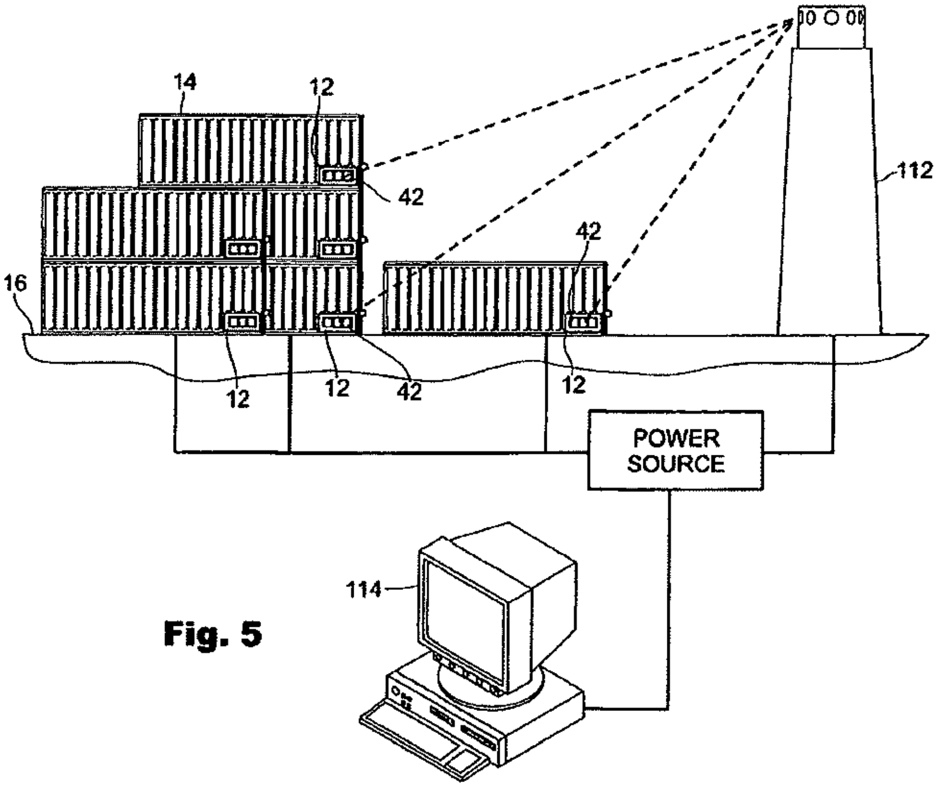


Fig. 5

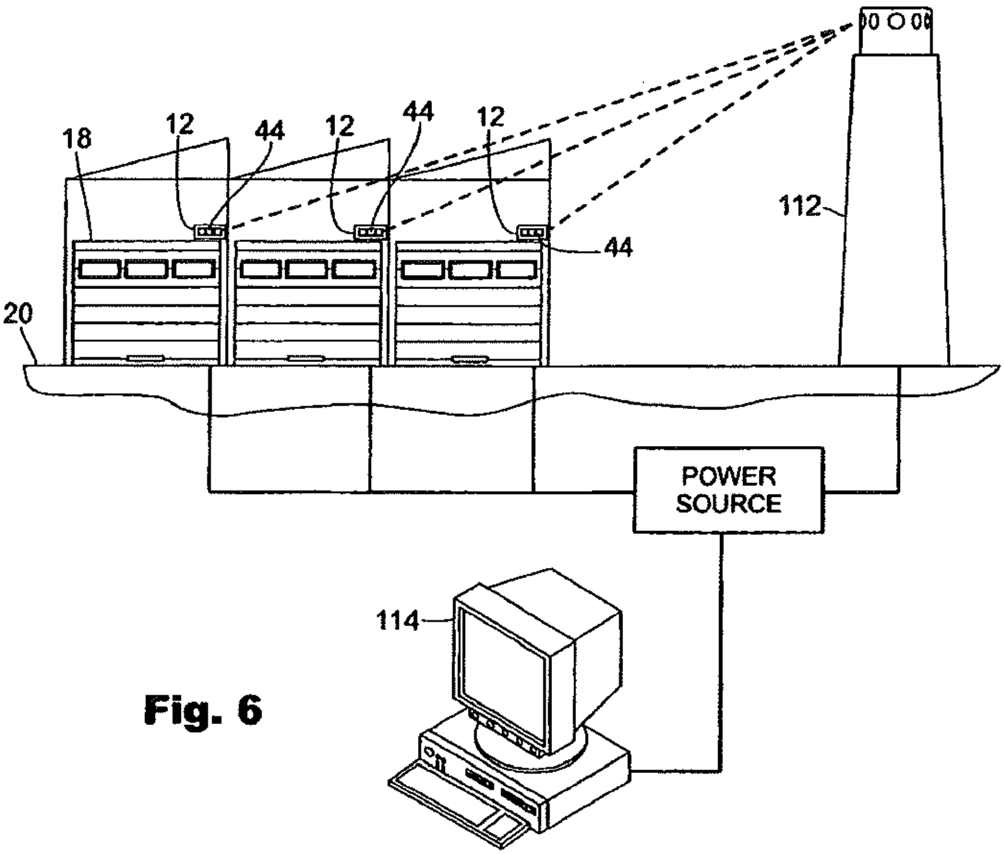


Fig. 6

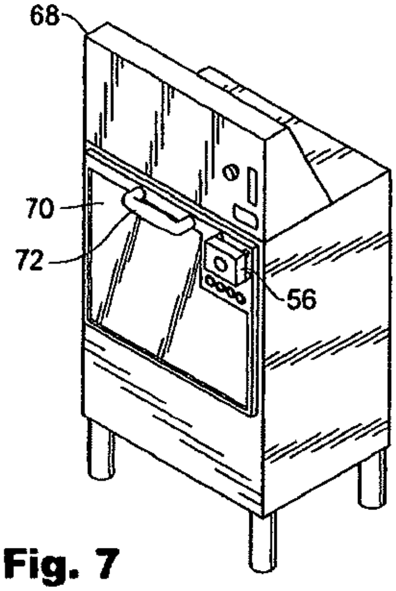


Fig. 7

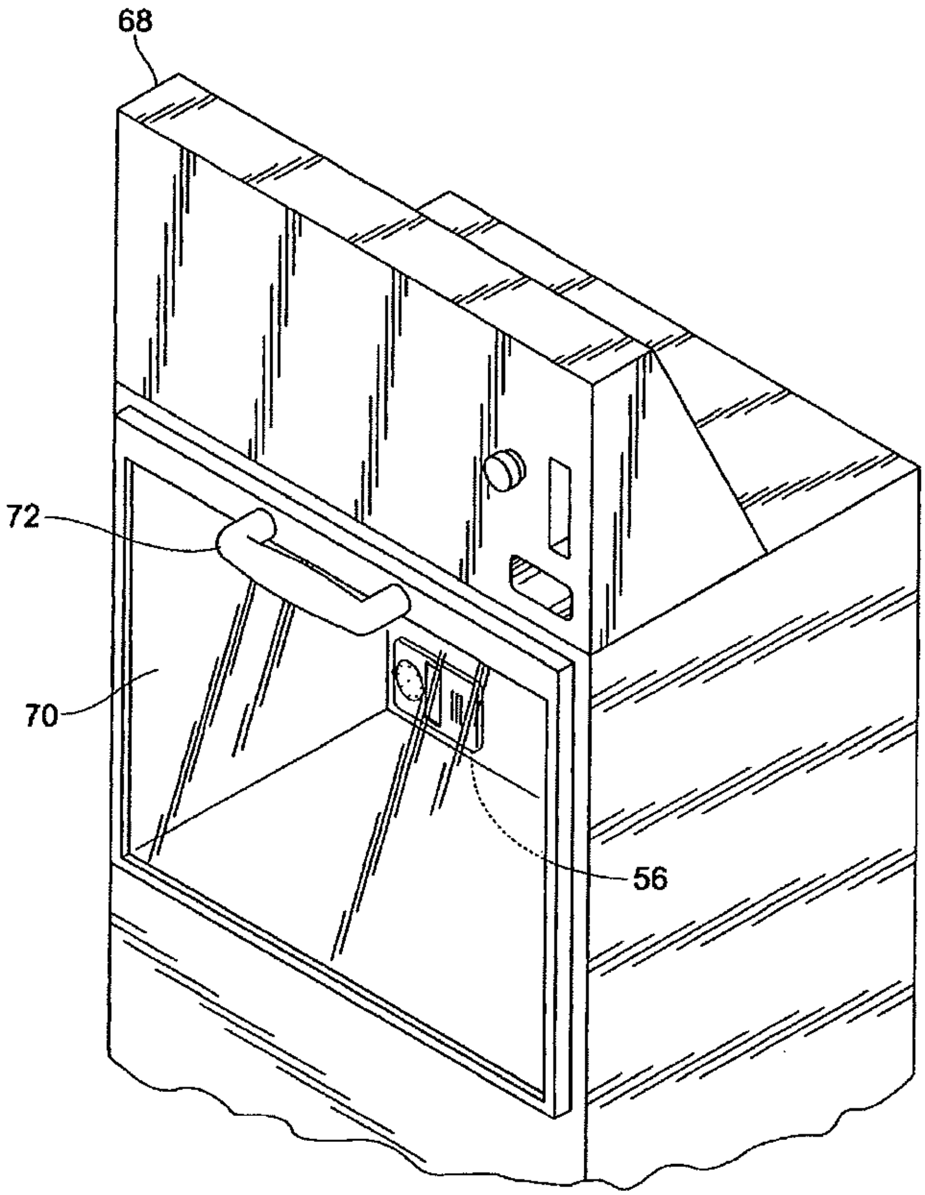


Fig. 8

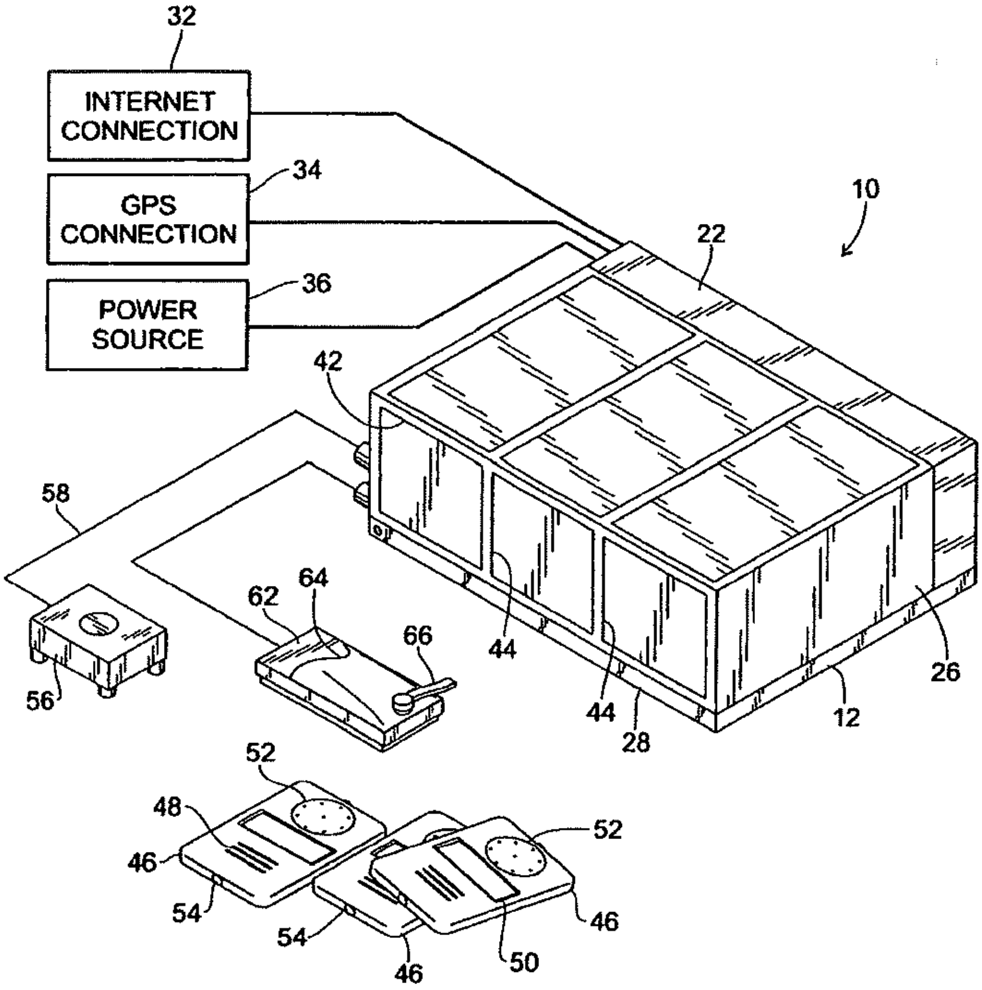

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
42
58
62
64
66
44
44
28
12
26
56
52
48
46
54
54
46
50
52
46

Fig. 9

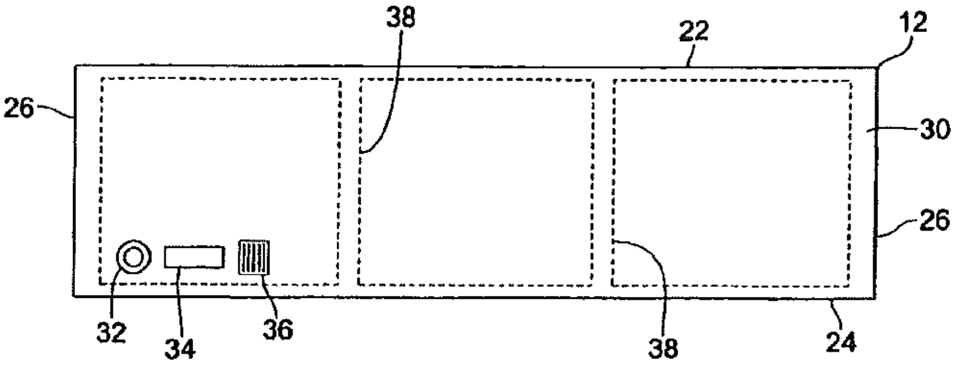

38
22
12
26
30
26
32
34
36
38
24

Fig. 10

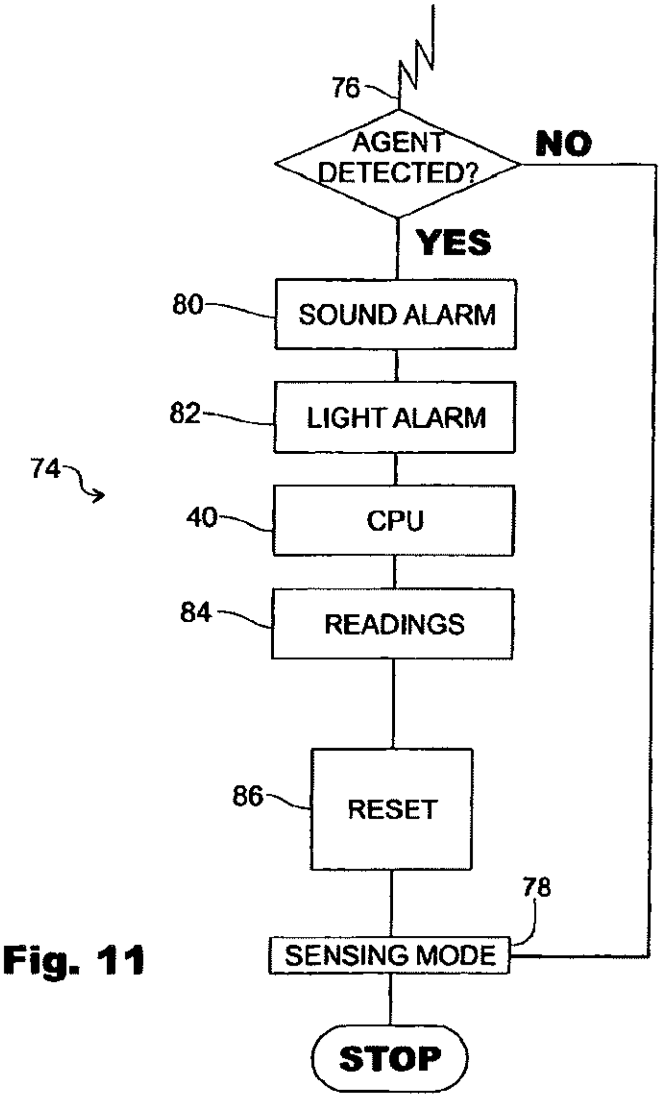

76
AGENT DETECTED?
NO
YES
80
SOUND ALARM
82
LIGHT ALARM
74
40
CPU
84
READINGS
86
RESET
78
SENSING MODE
STOP

Fig. 11

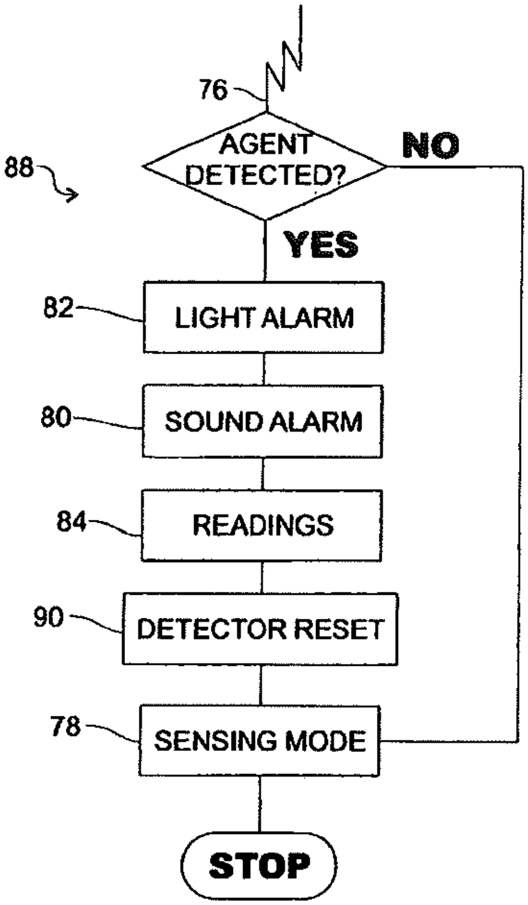

76
88
AGENT DETECTED?
NO
YES
82
LIGHT ALARM
80
SOUND ALARM
84
READINGS
90
DETECTOR RESET
78
SENSING MODE
STOP

Fig. 12

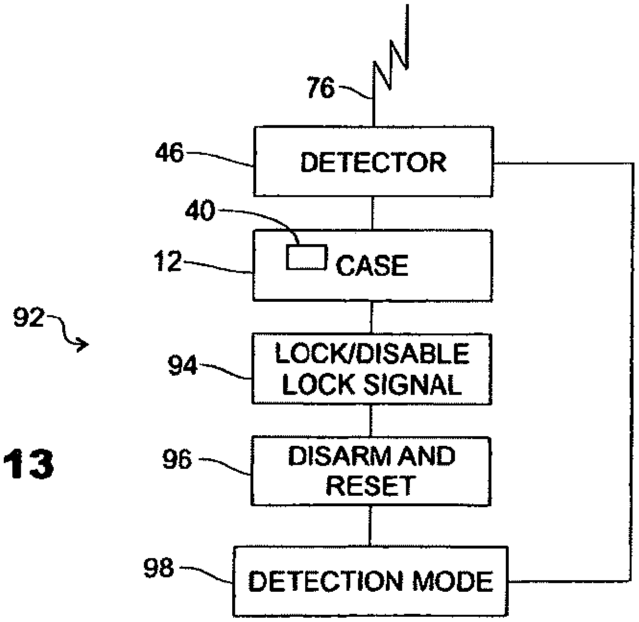

76
46
DETECTOR
40
12
CASE
92
94
LOCK/DISABLE LOCK SIGNAL
96
DISARM AND RESET
98
DETECTION MODE

Fig. 13

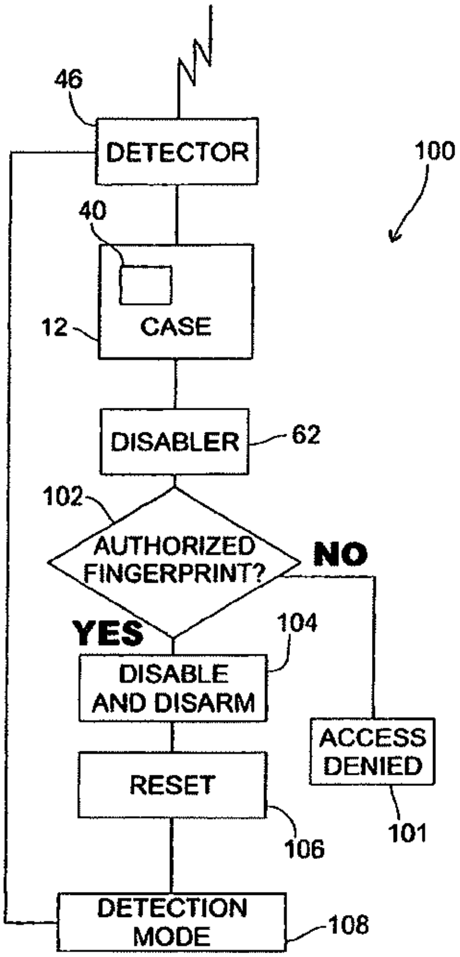

46
DETECTOR
100
40
12
CASE
DISABLER
62
102
AUTHORIZED FINGERPRINT?
NO
YES
104
DISABLE AND DISARM
ACCESS DENIED
RESET
106
101
DETECTION MODE
108

Fig. 14

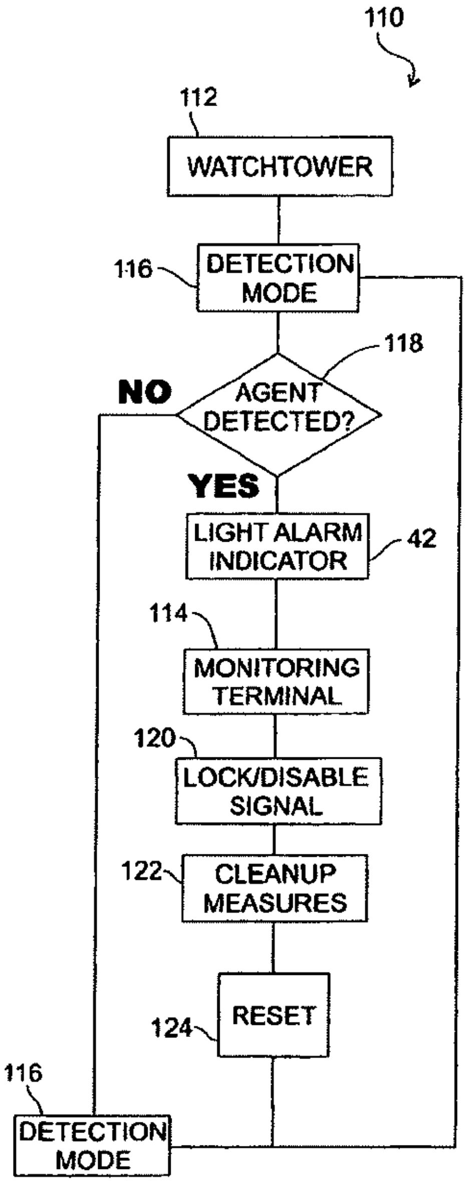

110
112
WATCHTOWER
116
DETECTION MODE
118
NO
AGENT DETECTED?
YES
LIGHT ALARM INDICATOR
42
114
MONITORING TERMINAL
120
LOCK/DISABLE SIGNAL
122
CLEANUP MEASURES
124
RESET
116
DETECTION MODE

Fig. 15

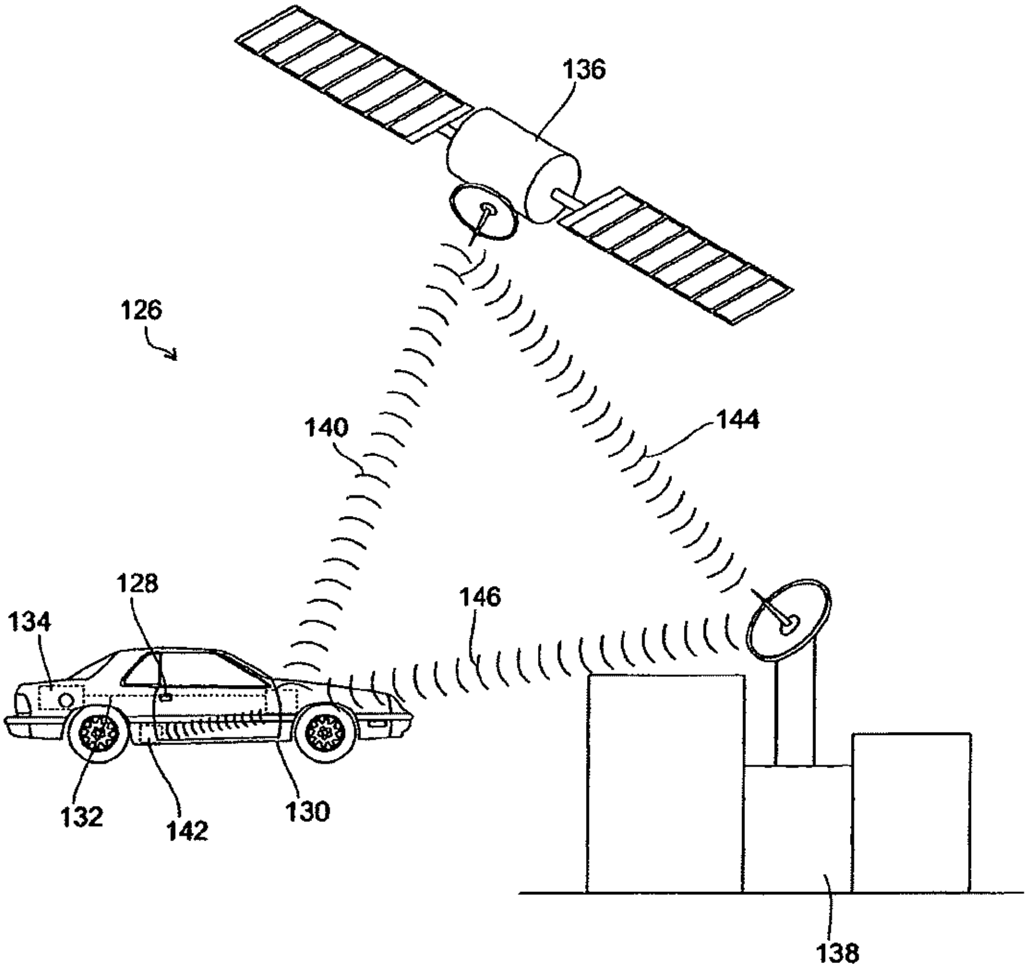


Fig. 16

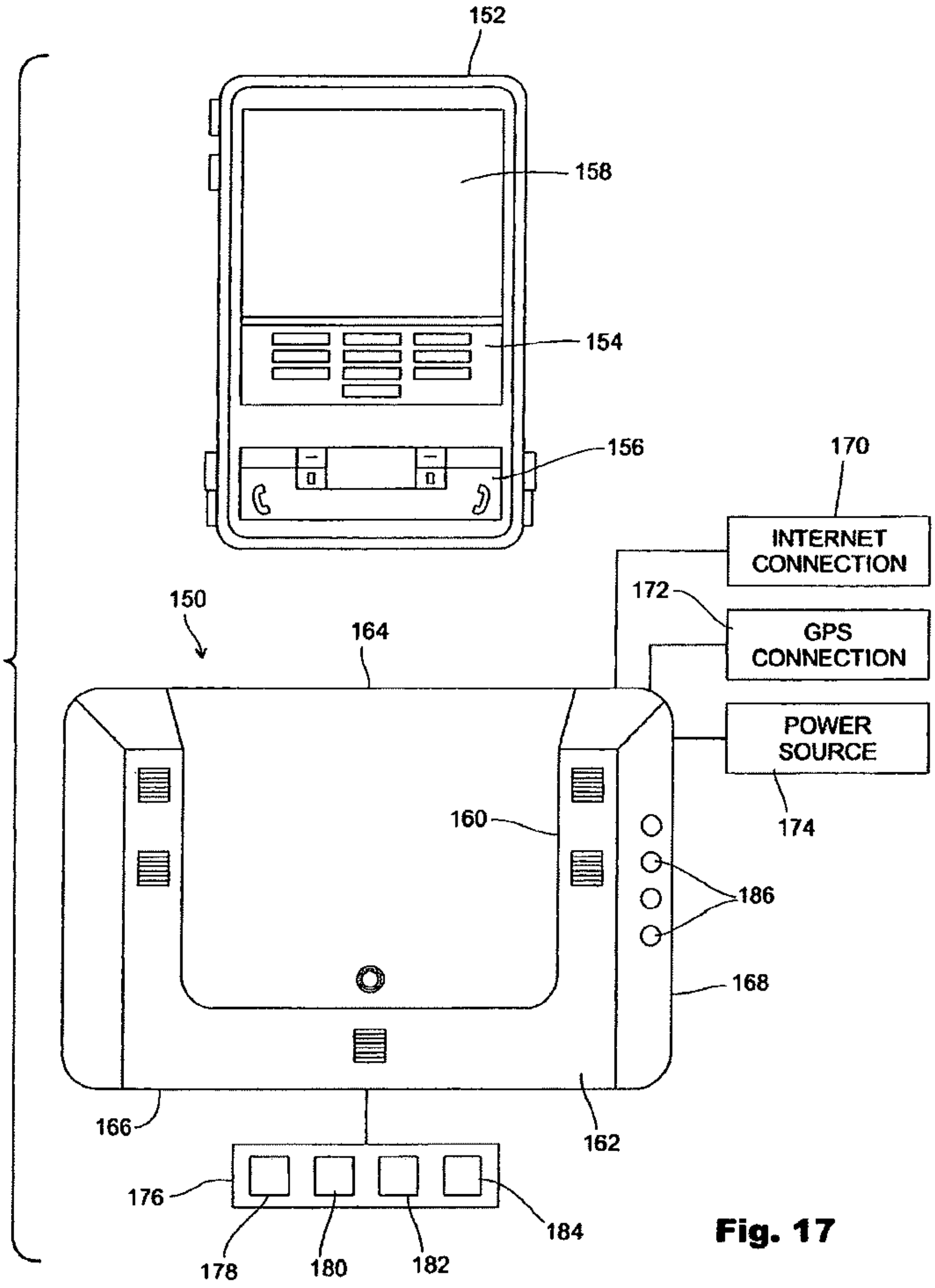

152
158
154
156
170
INTERNET CONNECTION
172
GPS CONNECTION
POWER SOURCE
174
150
164
160
186
168
166
162
176
178
180
182
184

Fig. 17

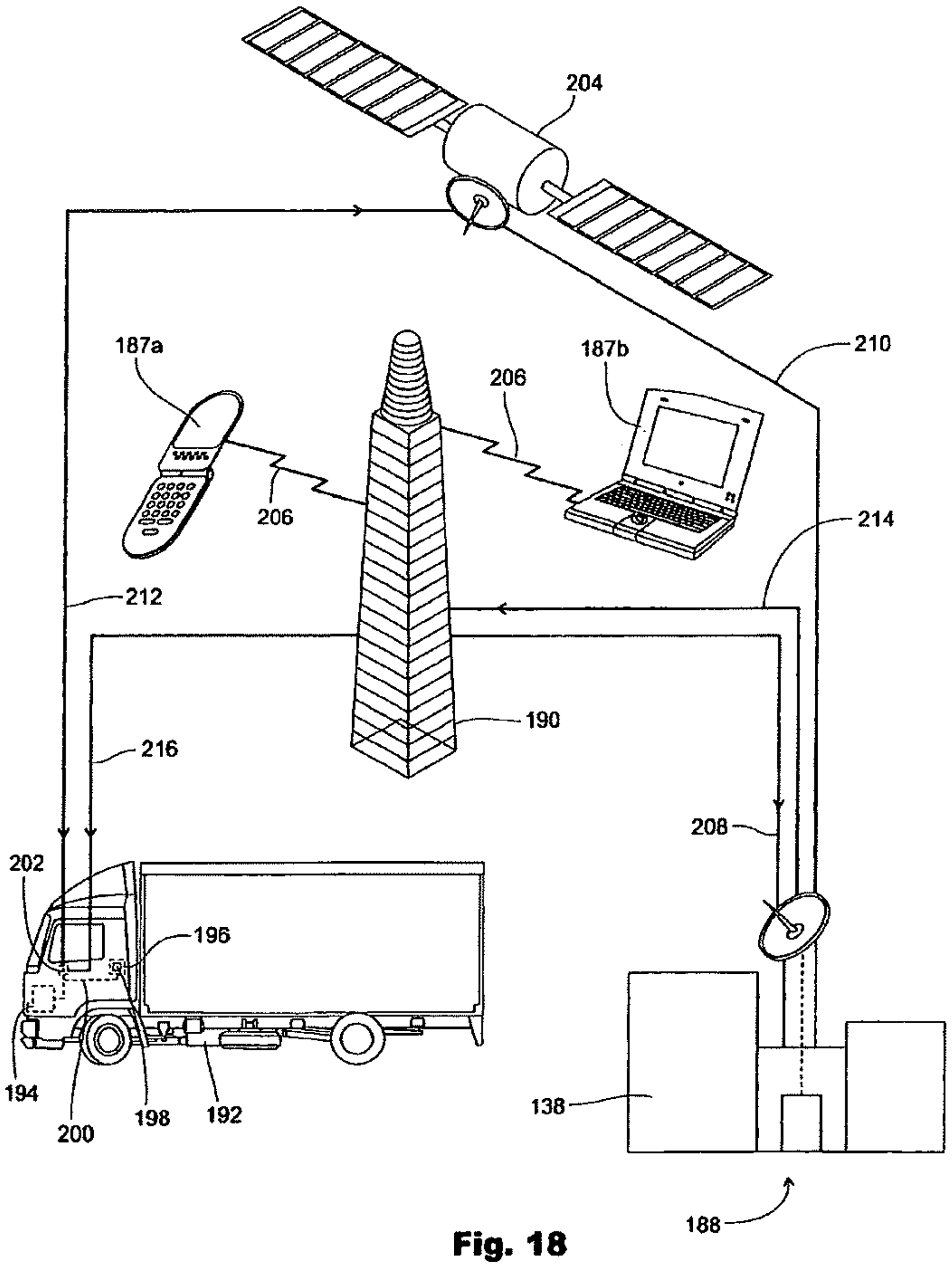

204
187a
206
187b
210
206
214
212
216
190
208
202
196
194
200
198
192
138
188

Fig. 18

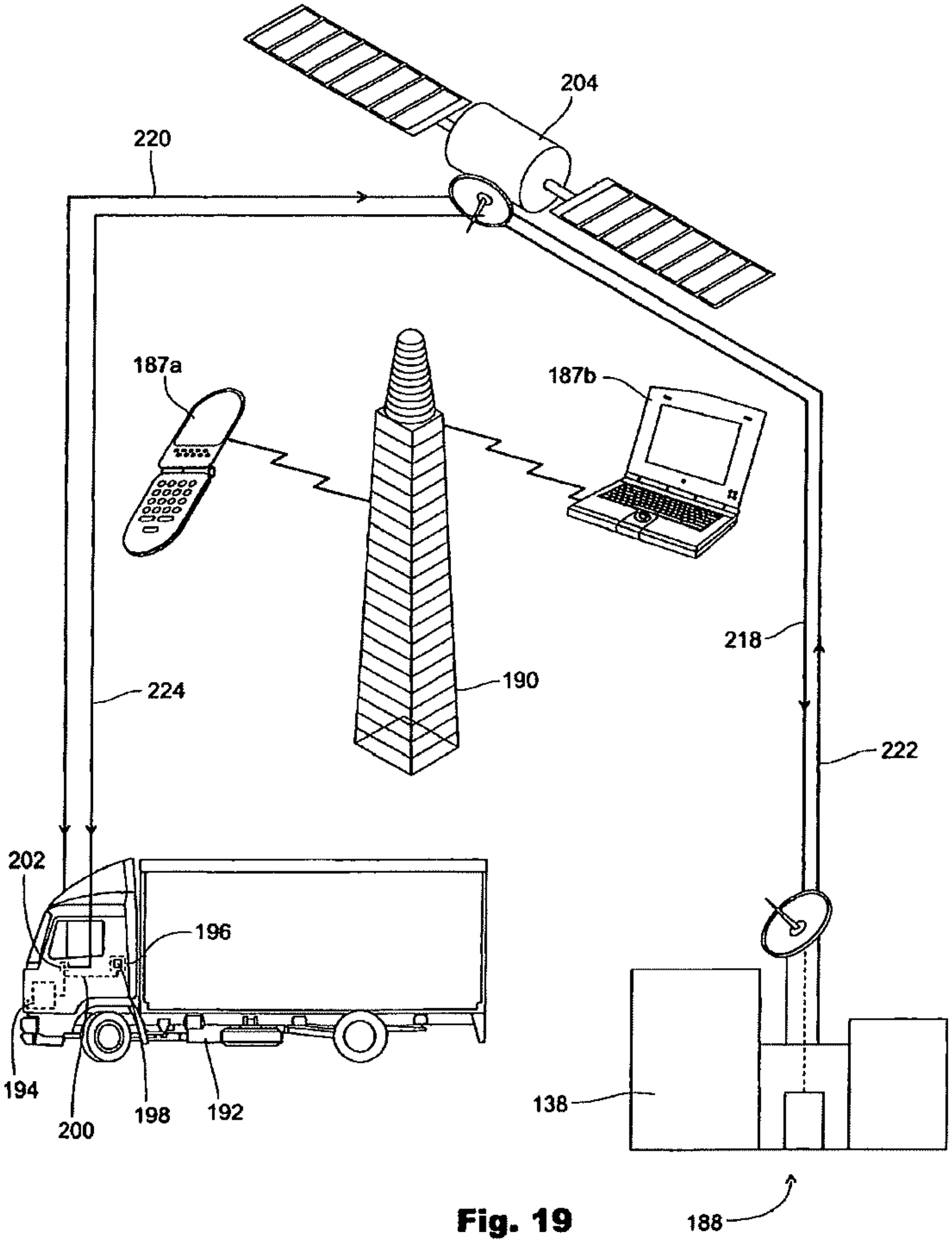

204
220
187a
187b
218
224
190
222
202
196
194
200
198
192
138
188

Fig. 19

MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM

This application is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 14/021,693 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Sep. 9, 2013 that issued on Aug. 4, 2015 as U.S. Pat. No. 9,096,189, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 9,096,189 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 13/288,065 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Nov. 3, 2011 and that issued on Sep. 10, 2013 as U.S. Pat. No. 8,531,280, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 13/288,065 that will issue as U.S. Pat. No. 8,531,280 is a divisional application and claims the filing date and benefit of U.S. patent application Ser. No. 12/802,001 titled "Multi Sensor Detection, Stall to Stop, and Lock Disabling System" filed on May 27, 2010, now U.S. Pat. No. 8,334,761, the entire contents and complete subject matter of which are incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 12/802,001 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 12/657,356 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Jan. 20, 2010, now U.S. Pat. No. 8,106,752 and incorporates the entire contents and complete subject matter therein by reference in their entirety for all purposes. U.S. Pat. No. 8,106,752 is a continuation of and claims priority to U.S. Pat. No. 7,636,033. U.S. Pat. No. 7,636,033 is a continuation-in-part of and claims priority to U.S. Pat. No. 7,385, 497. U.S. patent application Ser. No. 13/288,065 that issued as U.S. Pat. No. 8,531,280 also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/657,356, now U.S. Pat. No. 8,106, 752 herein by reference for all purposes. The present application also claims the filing date and benefit of and incorporates the entire contents of U.S. Pat. Nos. 8,531,280; 8,334,761; 8,106,752; 7,636,033; and 7,385,497 by reference herein in their entireties for all purposes.

FIELD OF THE INVENTION

The present invention pertains to anti-terrorist detection and prevention systems, and more particularly pertains to a disabling lock mechanism combined with a chemical/biological/radiological detection system for use with products grouped together by similar characteristics in order to prevent unauthorized entry, contamination and terrorist activity.

BACKGROUND OF THE INVENTION

Terrorist activity is a continuous, daily, worldwide threat to the stability, prosperity, security and peace within nations and between and among nations. Its danger lies in its arbitrary destructiveness as much as in its unpredictability, and the constant threat of terrorist activity compels measures and actions that cause strain and contention in free, democratic societies as security concerns and civil liberty concerns must be balanced so that both public safety and civil liberties are maintained. Safety and security concerns can be addressed through numerous proactive steps and measures, many of which cause only minimal interference with and disruption of the daily routines of work, travel, commerce

and entertainment. However, because modern industrial societies afford almost limitless places, locations, and opportunities for terrorist activities, no safety measure or security protocol will be foolproof, but many security measures, systems and protocols can be implemented that greatly minimize specific threats through fingerprint identification procedures, chemical, biological, and radiological hazard detections, bomb and explosive detection, and controlling the access to everything from shipping containers to school lockers. Thus, the prior art discloses a wide range of security measures and systems.

For example, the Fishbine et al. patent (U.S. Pat. No. 4,792,226) discloses an optical fingerprinting system that includes an optics/processor unit, a video monitor, a data terminal, and a printer for collecting and storing data characteristics of all ten individual fingerprints for printing demographic information and fingerprint images as desired on a standard booking or applicant card.

The Schiller patent (U.S. Pat. No. 4,544,267) discloses a finger identification unit that includes a fingerprint scanning apparatus using a collimated beam of light to interrogate the fingerprint of a finger placed against a platen so that successive scan positions produce signals containing fingerprint information.

The Fishbine et al, patent (U.S. Pat. No. 5,222,152) discloses a portable fingerprint scanning apparatus for optically scanning and recording fingerprint images and wirelessly transmitting such images to a mobile processing unit for verification and background checking.

The Lougheed at al. patent (U.S. Pat. No. 5,233,404) discloses an optical scanning apparatus that uses a linear charge coupled device (CCD) for recording the image of a fingerprint on the viewing surface.

The Groger et al. patent (U.S. Pat. No. 5,766,956) discloses a diode laser based sensor for undertaking optical, chemical, immunological or nucleic acid-based assay or other chemical analysis.

The Feldman patent (U.S. Pat. No. 5,938,706) discloses a multi element security system for preventing the unauthorized use of an automotive vehicle, and which includes numerous locking and control features interconnected to an onboard cpu.

The Bowker et al. patent (U.S. Pat. No. 5,963,657) discloses a safety access control for doors, handles, locks, etc., wherein the surface relief of a finger is read and verified to either allow or prevent access by the individual to the door, handle, lock, etc.

The Bonder et al. patent (U.S. Pat. No. 6,078,265) discloses a fingerprint identification security system wherein a key lock operated security system utilizes the fingerprint of the individual to control user access to the security system, such as the ignition system of an automotive vehicle.

The Anzai et al. patent (U.S. Pat. No. 6,271,745 B1) discloses a keyless authorization system for use of a motor vehicle that includes fingerprint reading units located on the exterior or interior of the motor vehicle and which is coupled to a control unit for scanning, comparing and matching fingerprints to allow or disallow access to the motor vehicle.

The Hwang patent (U.S. Pat. No. 6,374,652 B1) discloses a fingerprint-activated doorknob in which a detecting sensor for a fingerprint is placed on the doorknob for measuring and searching the fingerprint against previously stored fingerprint inputs to control access to the door.

The Vor Keller et al. patent (U.S. Pat. No. 6,588,635 B2) discloses a safety holster for a firearm that includes a pivotally mounted retaining member and a fingerprint sensor for scanning fingerprint information so that only authorized users can withdraw the firearm from the holster.

The Cordery et al. patent (U.S. Pat. No. 6,613,571 B2) discloses a method and system for detecting biological and chemical hazards in the mail that includes sensors placed within the mail box for sampling and testing ambient air and so that mail can be safely transported through the mail system.

The Nagata patent (U.S. Pat. No. 6,628,213 B2) discloses a coding method for digital signal coding and decoding that includes a CMI (code-marked inversion) method of signal coding.

Nonetheless, despite the ingenuity of the above devices, methods, and systems, there remains a need for a multi-detector and disabling lock system for use with various types of products collected together by common characteristics into product groupings for detecting chemical, biological and radiological agents and compounds and for selectively disabling and activating the product locks thereby preventing unauthorized entry and further contamination and preventing and thwarting terrorist activities.

SUMMARY OF THE INVENTION

The present invention comprehends a chemical/biological/radiological detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping **1** include, but are not limited to, cargo containers, shipping containers, tractor trailers, snail carriers, mail boxes and lockers; while the products grouped into what may be referred to as Product grouping **2** include, but are not limited to, chemical, biological, radiological, and nuclear detectors, motion sensors and door sensors. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The multi sensor detection and lock disabling system includes a detector case sized to fit in, upon or adjacent any of the aforedescribed products for detecting harmful and dangerous chemical, biological, and radiological agents, compounds and elements. In addition, the multi sensor detection and lock disabling system is capable of transmitting a signal to lock or disable a lock on the product, and is also capable of transmitting signals to a monitoring computer terminal or PC so that appropriate defensive and safeguarding actions can be undertaken and an authorized individual can disarm and reset the locking system and the multi sensor detection system. The detector case includes a power source (battery or electrical), interior compartments, Internet and GPS connections and a cpu interconnected with the Internet and GPS connections, and also interconnected with one or more off site monitoring computer terminals or PCs. The detector case includes one or more light alarm indicators that are externally visible and that light up when the chemical, biological, or radiological agent or compound is detected, and the light alarm indicators (which can be indicator lights or panels on the front of the detector case) can be color coded for denoting the specific agent or compound detected, i.e., separate and distinct colors for indicating detection of the chemical, biological, or radiological agent or compound.

The detector case is designed to hold within the interior compartments one or more interchangeable detectors, and each detector is adapted and set up to sample a specific compound or agent. Each detector includes a sound alarm, a sensor, a light alarm, and a readings panel, and is electrically interconnected (either by wire or wirelessly) to the cpu of the detector case so that information regarding the detection of the particular agent or compound can be conveyed from the detectors to the detector case cpu. Each detector can also be used as a manual, stand-alone hand held scanner.

The multi sensor detection and lock disabling system can be interconnected to a surveillance watchtower, as well as monitoring computer terminals or PCs, with the watchtower scanning shipping and cargo crates and containers being prepared for shipment or sitting for extended periods of time on a dock or at a port, at a railway site, or at an industrial storage facility. The watchtower will scan the cargo and shipping crates and containers for the light alarm indicators on detector cases that are mounted in or upon the crates and containers, and thus continuous security surveillance of the crates and containers can be maintained.

An enhanced version of the multi sensor detection and lock disabling system can be employed to prevent car and vehicle bombings. Coupling the multi sensor detection and lock disabling system with satellite service will enable the detection system to detect explosives and transmit an alert signal by satellite to monitoring equipment at a monitoring site. Upon receiving the alert signal at the monitoring site the monitoring equipment activates a stall-to-stop process for disabling the air, fuel, electrical and/or computer system of the vehicle. Moreover, upon receiving the alert signal at the monitoring site the car or vehicle will be locked by transmission of a satellite signal that disables the vehicle's electrical and ignition system thereby preventing escape of the terrorist.

It is an objective of the present invention to provide a multi sensor detection and disabling lock system for securing news racks and vending machines in order to prevent theft, unauthorized use and terrorist activity.

It is another objective of the present invention to provide a multi sensor detection and disabling lock system for preventing terrorist activity by using products grouped together by common features in several product groupings such as design similarity, similarity in the presentation of security problems and similarity with regard to the presentation of solutions to preventing terrorist solutions.

It is still yet another objective of the present invention to provide a multi sensor detection and disabling lock system that is capable of disabling an existing lock or activating a lock inside any of the products of the product grouping lists when a detector or sensor of the system is activated.

It is still yet a further objective of the present invention to provide a multi sensor detection and disabling lock system wherein the disabling lock system prevents the unauthorized entry, access and further contamination of the products included in the several product groupings.

A still further objective of the present invention is to provide a multi sensor detection and lock disabling system that utilizes a multi-task device for preventing terrorist activity to vulnerable products that are collected or arranged by product grouping categories.

Yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system to secure cargos and containers, especially cargo and shipping containers, against chemical, biological, radiological and nuclear terrorist activity.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system capable of detecting chemical, biological and radiological agents and compounds.

Still yet another objective of the present invention is to provide a multi sensor detection and disabling lock system that includes interchangeable detectors that operate in conjunction to detect chemical, biological and radiological agents and compounds.

Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories.

Another objective of the present invention is to provide a multi sensor detection and disabling lock system that accurately and reliably detects harmful agents, compounds and elements, and prevents the placement and storage of weapons and bombs in the range of storage containers and facilities currently available.

Still, another objective of the present invention is to provide a multi sensor detection and disabling lock system wherein the interchangeable detectors that comprise part of the system can be used as stand-alone scanners.

These and other objects, features, and advantages will become apparent to those skilled in the art upon a perusal of the following detailed description read in conjunction with the accompanying drawing figures and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the primary features of the system which include a detector case, several interchangeable detectors, an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler;

FIG. **2** is a front elevation view of the multi sensor detection and lock disabling system of the present invention illustrating one of the interchangeable detectors first shown in FIG. **1**;

FIG. **3***a* is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one lock disabler to the lock of a product, such as a container, and disengaged from the lock of the container;

FIG. **3***b* is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the engagement of the lock disabler to the lock of the product for locking or disabling the lock of the product so that unauthorized access is prevented;

FIG. **4** is a side elevation view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case mounted to the product, such as the container, with the light alarm indicators externally visible;

FIG. **5** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of detector cases with a surveillance watchtower and a monitoring PC terminal;

FIG. **6** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the placement of detector cases upon containers different

from the containers of FIG. **5**, and wherein the detectors case are interconnected to a surveillance watchtower and a monitoring PC terminal;

FIG. **7** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one automatic/mechanical lock disabler to the lock of a standalone news rack;

FIG. **8** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating one interchangeable detector placed within the standalone news rack;

FIG. **9** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case having color coded front panels for specifically indicating the agents, compounds or elements that have been detected;

FIG. **10** is a rear elevation view of the multi sensor detection and lock disabling system of the present invention illustrating the GPS, Internet and power source connections;

FIG. **11** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector with the detector case and the steps undertaken by the system when an agent or compound is detected;

FIG. **12** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the sequence of steps undertaken by one detector when functioning as a standalone scanner for detecting an agent or compound;

FIG. **13** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector case with the automatic/mechanical lock disabler for activating the lock disabler upon detection by the system of an agent or compound;

FIG. **14** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating interconnection of the detector case with the fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public upon detection of the agent or compound;

FIG. **15** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the system with a surveillance watchtower and a monitoring PC or computer terminal for monitoring containers, such as shipping or cargo containers, that may sit for extended time periods on docks, at rail yards, and at industrial storage facilities;

FIG. **16** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the integration of the detection system with a satellite and monitoring equipment at a monitoring site for detecting explosives placed in a vehicle and then transmitting signals to the satellite and then to the monitoring site for disabling and locking the vehicle;

FIG. **17** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the features and elements of the detector case to a cell phone and cell phone case;

FIG. **18** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of a OPS satellite, a monitoring site and a cell phone tower for communicating to and with an electronic device such as a laptop computer or a cell phone for transmitting signals to a vehicle for activating an onboard stall-to-stop device for bringing the vehicle to a halt; and

FIG. **19** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the use of a GPS satellite in conjunction with the monitoring site and monitoring equipment to relay commands and signals to the cpu or transceiver of the vehicle for stopping or locking the vehicle in response to a signal that a certain type of event (detection of a bomb, engine failure or malfunction or unauthorized use) has occurred or is in process

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Illustrated in FIGS. **1-19** is a multi sensor detection and lock disabling system **10** for preventing terrorist activity by monitoring, detecting, and securing those critical areas, sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities that are vulnerable to terrorist activity as convenient places to store and plant explosives and bombs and spread biological, chemical or radiological agents and compounds, followed by the disposition of the multi sensor detection and lock disabling system **10** for monitoring, detecting, and securing the particular location or site. Vulnerable sites, locations, facilities and areas are nearly limitless in their variety; in order to categorize the protection the present invention provides an anti-terrorist product grouping strategy has been developed wherein products made from the same or similar material, products having the same or similar design, and products presenting the same or similar security problems are grouped together with the multi sensor detection and lock disabling system **10** for preventing terrorist activity. For example, two preferred product groupings can be Product Grouping I: cargo containers, shipping containers, cargo planes, freight train cars, tractor trailers, mail carriers (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans and utility vehicles. Product Grouping II: chemical detectors, biological detectors, radiological detectors, nuclear detectors, motion sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems. In addition to grouping products together by features, designs and materials, the multi sensor detection system **10** includes a lock disabling capability for disabling an existing lock or activating a lock on or inside any of the aforementioned products when a detector or sensor of the system is activated. The lock disabling feature is a crucial component of the invention in so far as it prevents unauthorized, unequipped or untrained individuals from gaining access and entry to the site and causing further contamination of the site.

As shown in FIGS. **1-10**, the multi sensor detection and lock disabling system **10** includes at least one—and preferably many—detector case **12** that can be placed in, on, upon or adjacent the product, such as the shipping containers **14** of FIGS. **4** and **5** resting upon a platform **16** or the cargo container **18** of FIG. **6** sitting upon a seaport dock or pier **20**. The detector case **12** includes a top **22**, a bottom **24**, a pair of opposed sides **26** and a front side or panel **28** and an opposite rear or back side **30**. The rear side **30** has connections or contacts that can include an Internet connection **32**, a GPS connection **34** and a power connection **36** for a power source. The power source for the detector system **10** can be any conventional battery or electrical source. The detector case **12** includes an interior chamber divided into a number of compartments **38** for holding therein agent or compound detection means hereinafter further described. A cpu **40** is mounted within the detector case **12** and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment. The front side **28** of the detector case **12** includes indicator means for visually indicating that a specific agent, compound or element has been detected. The indicator means can include color coded indicator lights **42** in panel form, as shown in FIG. **9**, with each indicator light panel **42** lighting up with a specific color corresponding to the detection of a specific agent or compound; or color coded indicator lights **44**, as shown FIG. **1**, that correspond to and individually light up on the detection of a specific agent or compound (chemical, biological, or radiological).

As shown in FIGS. **1**, **2** and **9-13**, the multi sensor detection and lock disabling system **10** includes a plurality of detectors **46** with each detector **46** adapted for and set up to sample for a specific agent or compound (biological, chemical, or radiological); and the detectors **46** are interchangeable for adapting to the needs and demands of future technology. The detectors **46** can also be used as standalone scanners. In the preferred embodiment of the invention, at least three detectors **46** are placed within the detector case **12** with one detector **46** for specifically sampling biological agents or compounds, one detector **46** for sampling chemical agents or compounds, and one detector **46** for sampling radiological agents or compounds. The detectors **46** are interconnected to the cpu **40** of the detection system **10** by conventional connections that can be wire or wireless for transmitting the appropriate signals to the cpu **40** upon detection of the particular agent or compound. As shown in FIG. **2**, each detector **46** includes on its front plate or facing surface a sound alarm indicator **48**, a readings panel **50** comprising a plastic shield and LED lights for displaying the various read-out messages, a sensor **52** for detecting the specific agent, element or compound, and a light alarm indicator **54** that can be color coded for each specific agent and which is externally visible when the detector **46** is used as a stand alone scanner. Each detector **46** includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the cpu **40** of the detector case **12**.

As shown in FIGS. **1**, **3***a*, **3***b*, **9**, and **13-15**, used in conjunction with the multi sensor detection and lock disabling system **10** is at least one automatic/mechanical lock disabler **56**—and depending upon the number of products being monitored there can be one lock disabler **56** for each product. The automatic/mechanical lock disabler **56** is physically connected to the detector case **12** by a wire or cable **58** for receiving signals therefrom for disabling an existing lock or activating a lock inside a product to prevent access to the product. By way of example, FIG. **3***a* shows the automatic/mechanical lock disabler **56** mounted—by any conventional means—to the lock **60** of the shipping container **14** shown in FIGS. **4** and **5** and connected by wire **58** to the cpu **40** of the detector case **12**. The lock disabler **56** is in the non-activated or disengaged state in FIG. **3***a*. FIG. **3***b* shows the automatic/mechanical lock disabler **56** mounted to the lock **60** of the shipping container **14** and in the activated or engaged state after detection of an agent or compound by the system **10** thereby for locking or disabling the lock **60** of the shipping container **14** and preventing unauthorized entry and access by unauthorized, untrained and unequipped individuals. In FIGS. **3***a* and **3***b* the lock **60** secures doors of the shipping container **14** that can be slidably or pivotably opened and closed.

In addition to the automatic/mechanical lock disabler **56**, the multi sensor detection and lock disabling system **10** can also utilize a fingerprint biometric lock with disabler **62** as shown in FIGS. **1** and **14**. The fingerprint biometric lock with disabler **62** is interconnected to the cpu **40** of the detector case **12** for receiving transmissions therefrom after detection of an agent or compound has occurred so that the lock on the product can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler **62** occurs when the fingerprint of the individual is placed on the fingerprint-matching pad **64**, and if a match occurs with a known fingerprint stored by the cpu **40**, then the individual can reset the fingerprint biometric lock with disabler **56** by turning the manual lock disabler **66**. The fingerprint biometric lock with disabler **62** is mounted to the lock of the product in a manner similar to the mounting of the automatic/mechanical lock disabler **56** that is shown in FIGS. **3** and **3***b*.

FIGS. **4** and **5** show one manner of disposition or placement of the detector case **12** in relation to the product, i.e., the shipping container **14**, with the color coded indicator lights **42** externally viewable; FIG. **5** shows a number of shipping containers **14** each equipped with a detector case **12** and integrated with elements hereinafter further described for continuously monitoring the shipping containers **14** as they sit for an extended period of time on the truck or rail platform **16**. FIG. **6** illustrates several cargo containers **18** sitting on the shipping dock or pier **20**, with each cargo container **18** having a detector case **12** mounted thereon and integrated with and monitored by elements shown in FIG. **5** and hereinafter further described.

FIG. **7** illustrates a typical product from product grouping **1** that is monitored by the multi sensor detection and lock disabling system **10** of the present invention; specifically, FIG. **7** shows a news rack **68** with one automatic/mechanical lock disabler **56** mounted to and interconnected with the locking mechanism of the news rack **68**. As long as there is no detection of any agent or compound, the lock disabler **56** is in the disengaged state, and the individual can deposit the coin amount in the chute and then freely open the glass panel **70** by the handle **72** for removing a paper. However, the lock disabler **56** would be activated upon detection of the harmful agent or compound and receipt of a signal from the cpu **40** for locking or disabling the locking mechanism thereby denying access to the interior of the news rack **68** from all untrained, unauthorized and unequipped individuals.

FIG. **8** illustrates one detector **46** disposed within the news rack **68** and which is visible through the panel **70** for detecting one specific agent, compound or element. The detector **46** functions as a stand-alone scanner and can be wirelessly interconnected to offsite monitoring equipment.

FIG. **11** illustrates a representative schematic **74** for describing the signal transmission process from the detector **46** to the cpu **40** of the detector case **12**. The external stimulus **76** would be the chemical, biological or radiological agent or compound. If there is no detection of the agent or compound, the detector **46** will stay in the sensing mode **78**. However, detection of the specific agent will trigger the sound alarm **80** and the light alarm **82**, and instant transmittal of a signal to the cpu **40**. The readings **84** can be stored by the cpu **40** for verification and future review and evaluation. After all the appropriate corrective and preventative

measures have been undertaken by the trained and authorized personal, and the site has been cleansed of the contamination, authorized and equipped personal can then reset **86** the system **10**.

FIG. **12** illustrates a representative schematic **88** for the detector **46** when used as stand-alone scanner. The detector **46** undergoes the same essential steps as illustrated in FIG. **11**, with the exception of the signal transmission to the cpu **40**. The detector **46** remains in detection mode **78** until an agent is detected, and then the various functions—light alarm **82**, sound alarm **80**, storage of readings **84**, and, after the appropriate security and safety steps have been carried out by authorized personal, detector reset **90** by authorized personal can occur thereby placing the detector **46** back in detection or sensing mode **78**.

FIG. **13** is a representative schematic **92** that illustrates the steps undertaken by the system **10** to lock or disable a lock, such as the lock **60** for the shipping container **14** shown in FIGS. **3***a* and **3***b*. Upon detection of the agent (chemical, biological, radiological) the alarm light indicators **42** or **44** will light up providing external indication that an agent has been detected. In addition, the system **10**—the cpu **40**—will transmit a lock/disable lock signal **94** to the automatic/mechanical lock disabler **56** to lock or disable the lock on the product, such as the lock **60** on the shipping container **14** of FIGS. **3***a*-**5**. This prevents unauthorized, unequipped, or untrained individuals from entering or gaining access to the product for which a dangerous and perhaps lethal agent has been detected. After the proper authorities and authorized personal have been notified and all the appropriate security, preventative and clean up measures have been undertaken, the authorized individual can perform the disarm and reset function **96** for the system **10** placing the system **10** in back in the detection mode **98**.

FIG. **14** is a representative schematic **100** illustrating the use of the fingerprint biometric lock with disabler **62** with the system **10**. Upon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the cpu **40** would then transmit a signal to the fingerprint biometric lock, with disabler **62** to lock or disable the lock on the product, such as the lock **60** on the shipping containers **14** shown in FIGS. **3***a*-**5**. The shipping containers **60** would remain locked and in an access denied mode **101** should an attempt be made to gain access to the container **60** by opening the lock **60** with an unauthorized fingerprint. However, a fingerprint that matches stored and authorized fingerprints **102** would indicate an authorized individual, and would allow the individual to disable and disarm **104** the lock **60** of the shipping container **14**. The fingerprint biometric lock with disabler **62** would then be reset **106** after the appropriate safety, cleanup, and protection measures are completed, and the system **10** would be reset and placed back in the detection mode **108**.

FIG. **15** is a schematic representation **110** that illustrates the integration of a surveillance watchtower **112** and a monitoring terminal or PC **114** for monitoring products such as the shipping containers **14** or cargo containers **16** that sit for extended periods of time of docks, piers **20**, truck terminals, rail yards, shipping platforms **16** and industrial sites as shown in FIGS. **5** and **6**. The watchtower **112** would maintain continuous surveillance over a number of shipping containers **60**, for example, with detector cases **12** mounted in or on each container **14** and set in detection mode **116** with one or more detectors **46** disposed in each detector case **12**. The watchtower **112** would continuously scan for light alarm indicators **42** and **44** on the products, such as the containers **14** or **18**, and the watchtower **112** would be interconnected and integrated with the monitoring terminal or PC **114**. Upon detection **118** of an agent or compound in one or more of the shipping containers **14**, the appropriate light alarm indicators **42** or **44** would light providing visible confirmation of the detection of the specific agent or compound. The cpu **40** would transmit a lock/disable signal **120** to the lock **60** on each respective shipping container **14** to lock or disable the lock **60** thus preventing access to that respective shipping container **14**. In addition, signal transmissions would be sent to the monitoring terminal or PC **114** (which could be off site) thereby alerting authorized security personal of the contamination event. With the information received at the monitoring terminal **114**, authorized personal would then be notified and dispatched to the area to undertake the appropriate safety and cleanup measures **122**. Such measures would also include disarming the lock disabling system in order to gain access to the shipping container **14**. After all the cleanup and security measures are completed by the trained and properly equipped authorities, the detection system and the lock disabling feature would reset **124** and the detection system would again be placed in detection mode **116**.

FIG. **16** is a schematic representation **126** that illustrates an enhanced version of the multi sensor detection and lock disabling system **10** for preventing car and vehicle attacks and bombings. The lock disabling system **10** would be interconnected to the locking system and mechanism **128** of the vehicle **130**. In addition, a stall to stop disabling link **132** can be made with the fuel, air, and electrical system **134** of the vehicle **130**. The enhanced version incorporates a satellite **136** for signal receipt and transmission from the vehicle **130** in which the detector system **10** is placed to a monitoring site and monitoring equipment **138**. As shown in FIG. **16**, a detection signal **140** would be sent to the satellite **136** by the detection system **10** upon detection of a bomb or explosive **142** hidden in the vehicle **130**. The satellite **136** would then transmit an alert signal **144** to the monitoring site **138** with the signal **144** containing the relevant data to evaluate the nature of the threat. The monitoring site **138** would then transmit a stall to stop signal **146** to the detection system **10** to lock the vehicle **130** and/or disable the electrical system of the vehicle **130** thereby disabling the vehicle **130**, preventing access to the vehicle **130** by locking the vehicle **130**, and preventing any terrorist in the vehicle **130** from escaping.

The detector case **12** can be modified and adapted for inclusion with cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, and briefcases. In addition, the basic monitoring terminal or PC **114**, as shown in FIGS. **5** and **15**, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring.

The system **10** and the watchtower **112**, along with the satellite **136** and the monitoring site **138** can be adapted or incorporated with cell phone towers and satellites for use with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu **40**, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween. The aforementioned telecommunication and radio communication means can be interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships and airplanes, and which is reported stolen, experiences a loss of brakes, or a

bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted to the vehicle and which detection causes an automatic signal transmission or a signal transmission is activated when a call is made to the monitoring station by an authorized person. The authorized individual includes but is not limited to the owner, pilot, conductor, captain, police highway patrol, security guard and military personnel to the monitoring equipment for activating a vehicle slowdown or stall-to-stop disabling system that similar to the disabling system **126** shown in FIG. **16**, or incorporating features of the system **126** shown in FIG. **16**, from the monitoring equipment to the vehicle. The activation of the stall-to-stop disabling means or the vehicle slowdown disables or engages the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.

In addition, the basic stall-to-stop disabling means or the vehicle slowdown means and device can be adapted, modified or designed to include: an open bust or open platform for integrating any new and innovative technology; warning lights indicators; sound alarm indicators; voice alarm indicators; a cell phone to transmit to the vehicle a signal for slowing and halting the vehicle; and a lock disabling system or means to lock a thief or terrorist inside the vehicle after a transmission is received or sent. Open bust or open platform also refers to the compatibility of the detector case **12**, or the incorporation of its features in cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, briefcases, and suitcases, etc., with other communication, transmission and surveillance systems whereupon the detector case **12**, and its features, can be seamlessly integrated with other new and emerging systems and technologies.

Thus, as shown more specifically in FIG. **17**, by way of a representative example the features and elements of the detector case **12** are shown as being incorporated into cell phone detector case **150** and associated cell phone monitor **152**. The cell phone monitor **152** includes the standard keypad functions **154** and more specialized system use (ring tone, email, photos, texting) functions **156** as well as a viewing screen **158**. The cell phone detector case **150** includes a recharging cradle or seat **160**, a front side **162**, a top **164**, a bottom **166**, and a pair of opposed sides **168**. At the back of the cell phone detector case **150** are connections, contacts, and ports for at least an Internet connection **170**, a GPS connection **172**, and a contact, plug, or port for a power source **174**. The power source for the cell phone detector case **150** can be any conventional rechargeable battery source or standard electrical power from a standard electrical receptacle or outlet.

As shown in FIG. **17**, the cell phone detector case **150** includes one or more sensor/detector units, cells, or components **176** built into and incorporated into the case **150**. The detector **176** includes generally disposed at the front **162** of the case **150** the following types of indicators: a sound alarm indicator **178**, a readings panel **180**, a sensor **182** for detecting one or more specific types of agents, elements, chemicals, compounds, etc., and a light alarm indicator **184**. The sensor/detector **176** will be interconnected to the power source **174**. In addition, mounted on and externally visible on the sides **168** or front **162** of the case **150** are a plurality of color coded indicator lights **186** with each fight **186** corresponding to a specific agent, element, chemical, compound, etc., and lighting up when that agent is detected by the sensor/detector **176**. The color coded indicator lights **186** will be electrically interconnected to the sensor/detectors **176** via any standard microprocessor. The cell phone detector case **150** and cell phone monitor **152** thus comprise a hand-held, easily portable and transportable detection means that is both effective and unobtrusive in its disposition and use.

FIGS. **18** and **19** illustrate representative examples of the integration of portable electronic communication or telecommunication devices such as a cell phone **187***a* and/or a laptop computer **187***b* with the monitoring equipment **138** located at a predesignated monitoring site **188**, and operating in conjunction with either a satellite and/or a cell phone tower **190** to transmit and receive signals and commands among each other and to a vehicle **192**, such as a truck, as part of a stall-to-stop disabling system for slowing and stopping the vehicle **192** and locking a thief, terrorist, or unauthorized individual in the vehicle **192** if needed. A wide range of events can trigger and initiate the stall-to-stop system and the locking or lock disabling system and mechanism, and the event doesn't have to be limited to the detection of a bomb or a chemical, biological, or radiological agent, element, or compound. The events can include, but is not limited to, detection of an engine problem to engine failure to the unauthorized use (stealing) of the vehicle **192**. The vehicle **192** includes an electromotive system **194** that comprises, among other components, an onboard computer(s), electrical, fuel and air systems, as well as brakes, ignition, steering, and transmission. Also integrated with and capable of communicating with the vehicle's **192** electromotive system **194** is a stall-to-stop system while a lock disabling mechanism **196** is able to engage and disengage or disable the vehicle's **192** locking mechanism **198** upon receipt of the appropriate commands via a lock disabling communication channel or link **200**. This link **200** can also accommodate the stall-to-stop system commands and signals, and thus is a multi-channel communication link. A CPU or a transceiver **202** is programmed to receive signals from the cell phone tower **190** and/or to a GPS satellite **204** and is interconnected with the stall-to-stop system and the lock disabling system **196** via link **200** for engaging the electromotive system **194** and actuating the lock disabling system **196** to stop the vehicle **192** and lock inside the vehicle **192** anyone such as a thief, terrorist or other unauthorized individual.

A representative example for stopping, disabling, and locking the vehicle **192** that utilizes the cell phone tower **190** wherein the activation and/or distress signal **206** originates from the cell phone **187***a* or the laptop **187***b* and such activation signal **206** travels to the cell phone tower **190** that is nearest the current location of the vehicle **192**. A signal **208** is then transmitted to the monitoring site **188** and specific monitoring equipment **138** that can also include but is not limited to cell phones, laptops, desktop PC's, notebook PC's and LCD monitors. The monitoring site **138** then communicates by signal **210** to the GPS satellite **204** that an original or activation signal has been received and then the GPS satellite **204** locates and communicates by multiplex signal **212** with the CPU or transceiver **202** on the vehicle **192** and exchanges information on the type of problem, situation, location, and vehicle speed. The monitoring equipment **138** then transmits a signal **214** to the cell phone tower **190** that communicates with the transceiver **202** and/or CPU of the vehicle **192** to initiate or execute any commands that will actuate the stall-to-stop disabling link **200** and lock disabling system **196** for bringing the vehicle **192** to a halt and actuating the vehicle's **192** locking mechanism **198** for locking the thief, terrorist, or other unauthorized person inside the vehicle **192** if needed.

FIG. **19** illustrates a representative example wherein the stall-to-stop system and the lock disabling system **196** are utilized in conjunction with the GPS satellite **204**. In FIG. **19** a signal has traveled to the satellites nearest the vehicle's **192** current location and then the signal **218** has traveled to the monitoring equipment **138** and monitoring site **188** which can include but is not limited to satellite cell phones, satellite monitors, cell phones, laptops, desktop PC's, notebook PC's, and LCD monitors. The UPS satellite **204** then locates and communicates with the CPU and/or transceiver **202** on the vehicle **192** via a multiplex (two-way) signal **220** in order to exchange information on such distress and danger event parameters as the specific problem situation, location, and vehicle speed. The monitoring equipment **138** then transmits a signal **222** back to the GPS satellite **204** that in turn communicates via another signal **224** with the CPU and/or transceiver **202** to execute any commands to the stall-to-stop system for executing the disengagement of the vehicle's **192** electromotive system **194** for bringing the vehicle **192** to a halt and for actuating the lock disabling system **196** to direct the lock disabling link **200** to actuate the locking mechanism **198** thereby locking the vehicle **192** and anyone inside the vehicle **192**.

The present invention comprehends a chemical/biological/radiological/nuclearlexplosive/human/contraband detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping **1** (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars, United Parcel Services™ (UPS™), Federal Express™ (FedEx™), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans, unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and utility vehicles; the products grouped into what may be referred to as Product grouping **2** (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, door sensors, speed sensors, biometric sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems, detection of humans, detection of contraband, temperature, and shock levels; the products grouped into what may be referred to as Product grouping **3** (detector case; modified and adapted) include, but are not limited to, cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, eyeglass, briefcases, detector cases of locks, detector cases of tags, detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to; the products grouped into what may be referred to as Product grouping **4** (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, web servers, desktop personal computers (PCs), notebook personal computers (PCs), laptops, satellite cell phones, cell phones, Universal Mobile Telecommunications System (UMTS) phones, personal digital assistants (PDAs), liquid crystal display (LCD) monitors, and satellite monitoring, remote control key fobs, two-way communication key fobs, handhelds; the products grouped into what may be referred to as Product grouping **5** (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN). Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), General Packet Radio Services (GPRS). Global System for Mobile (GSM), Wideband Code Division Multiple Access (W-CDMA), Universal Mobile Telecommunications System (UMTS), Short Message Service (SMS); the products grouped into what may be referred to as Product grouping **6** (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature, the products grouped into what may be referred to as Product grouping **7** (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside or outside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

While the invention has been shown and described in a preferred embodiment, it will be apparent to those skilled in the art that numerous alterations, modifications, and variations will possible and practicable without departing from the spirit and scope of the invention as set forth by the appended claims.

The invention claimed is:

1. A multi sensor detection system capable of identifying, monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities vulnerable to terrorist activity that can be integrated with and interconnected to watchtowers to form a network, comprising:

at least one of an integrated watchtower, a fixed watchtower, a surveillance watchtower, a watchtower capable of scanning, a watchtower capable of monitoring, a watchtower equipped with sensors or a watchtower interconnected to a central monitoring terminal for sending signals thereto and receiving signals therefrom;

wherein the at least one watchtower is equipped with a remote video surveillance camera that provides at least one night vision means of surveillance or an infrared human detection means of surveillance capability and is integrated into a watchtower's remotely controlled system that can monitor, detect, track, and identify humans;

a communication device of at least one of a mobile communication device, a mobile communication unit, a

portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop personal computer (PC), a notebook personal computer (PC), a laptop, a satellite phone, a smart phone, a cell phone, a Universal Mobile Telecommunications System (UMTS) phone, a personal digital assistant (PDA), a liquid crystal display (LCD) monitor, a satellite, or a handheld, interconnected to a monitoring equipment for sending signals thereto and receiving signals therefrom;

a communication method of at least one of a Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), or central processing unit (CPU), used to interconnect the communication device to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a plurality of sensors for detecting or sensing humans that is at least one of a chemical human sensor, biological human sensor, radiological human sensor, infrared human detector, motion human detector, or image human detector, interconnected to or disposed within the multi-sensor detection system for sending signals thereto and receiving signals therefrom;

a mobile multi-sensor detection device that is at least one of a ground surveillance sensor, a surveillance radar sensor, a surveillance camera, or a stand-alone surveillance scanner, that is mounted in, on, or upon at least one of a car, a truck, a camper, a bus, a van, an unmanned aerial vehicle (UAV), an unmanned ground vehicle (UGV), or a utility vehicle, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a hand-held multi-sensor detection device that is capable of at least one of thermal imaging or infrared imaging for monitoring, detecting, tracking and identifying humans, that is controlled or operated by at least one authorized person who is an owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, or monitoring site and terminal personnel, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, wherein the authorized person manually initiates the signal to the monitoring equipment to alert upon the monitoring, detecting, tracking and identifying of the human;

whereupon, detection by the mobile multi-sensor detection device causes an automatic signal transmission to be sent to, or received from, any products in product grouping categories of storage and transportation, sensors, detector case; modified and adapted, monitoring and communication devices, communication methods, biometrics;

whereupon, detection of an unauthorized vehicle, an unauthorized driver or operator of a vehicle or mobile unit, a signal is sent from the communication device to the vehicle or mobile unit to stop, stall or slowdown the vehicle;

wherein, a communication device of at least one of a mobile communication device, a mobile communication unit, a portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop PC, a notebook PC, a laptop, a satellite phone, a smart phone, a cell phone, a UMTS phone, a PDA, a LCD monitor, a satellite, or a handheld, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, comprising a lock disabling mechanism that is able to engage (lock), and disengage (unlock) and disable (make unavailable) after a specific number of tries.

2. The multi sensor detection system of claim **1**, capable of identifying, monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities, further includes the identifying, monitoring, and detecting of terrorist, that is at least one of an illegal, radical, fanatic, activist, revolutionist or rebel.

3. The multi-sensor detection system of claim **1**, further includes a global positioning system (GPS) receiver adapted for communication with at least one satellite.

4. The multi-sensor detection system of claim **1**, further includes a navigation system adapted for communication with at least one of the surveillance watchtowers.

5. The multi-sensor detection system of claim **1**, capable of forming a wired or wireless sensor network.

6. The multi-sensor detection system of claim **1**, capable of forming a mesh network for redundancy.

7. The multi-sensor detection system of claim **1**, capable of transmitting identification data, location data, power source data, and sensor data.

8. The multi-sensor detection system of claim **1**, capable of being embedded into; placed in, on, or adjacent to at least one of the products in the product grouping categories or an area targeted for monitoring.

9. The multi-sensor detection system of claim **1**, capable of sending signals thereto and receiving signals therefrom to engage (lock), disengage (unlock) and disable (make unavailable) a lock after a specific number of tries that is interconnected to the multi sensor detection system or monitoring equipment.

10. The multi-sensor detection system of claim **1**, capable of transmitting biometric and authentication data include, but is not limited to, at least one of fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

11. The multi-sensor detection system of claim **1**, interconnected with a camera to view the environment in real-time or to store the data for transmission and review at a later time.

12. The multi-sensor detection system of claim **1**, interconnected with a camera; light and video sensors to allow the user to view the environment from at least one of a cell phone, smart phone, PDA, handheld, laptop, desktop, workstation or monitoring site.

13. A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:

at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;

at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;

a receiver for receiving signals, data or messages from at least one of the multi-sensor detection device, the maritime cargo container, the cell phone detection device, or the locking device;

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;

the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock locking devices, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;

wherein the communication device receives a signal via any of one or more products in any product grouping categories;

wherein the at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection is capable of signal communication with the transmitter, the receiver of the communication device, or transceivers of the products;

wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;

wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, long range radio frequency (RF), and short range radio frequency (RF).

14. Monitoring equipment of at least one of products grouped together by common features in a product groupings category of design similarity comprising a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to a product for communication therebetween, the monitoring equipment comprising:

at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the monitoring equipment;

at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;

a receiver for receiving signals, data or messages from at least one of the multi-sensor detection device, maritime cargo container, the cell phone detection device;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;

monitoring equipment of at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the monitoring equipment, is interconnected to a product equipped to receive signals from or send signals to the lock disabling mechanism that is able to engage, disengage, or disable the lock, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;

wherein the monitoring equipment is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;

wherein the at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection is in signal communication with the transmitter, the receiver of the monitoring equipment, or transceivers of the products.

15. Monitoring equipment of at least one of the products grouped together by common features in a product groupings category of design similarity comprising a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to a product for communication therebetween, the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a microprocessor for executing and carrying out the instructions of a computer program or application which is specifically targeted at the networking application domain, for communication between the monitoring equipment and at least one of a multi-sensor detection device, a maritime cargo container device, or a locking device;

a transmitter for transmitting signals and messages to at least one of the multi-sensor detection device, the maritime cargo container device, or the locking device;

a receiver for receiving signals, data or messages from at least one of the multi-sensor detection device, the maritime cargo container device or the locking device, wherein the signals, data or messages are of agents of an item of interest (IOI);

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or GPS connection;

the monitoring equipment is at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the monitoring equipment, is capable of the activation or deactivation of at least one of the multi-sensor detection device, the maritime cargo container device or the locking device;

wherein the at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, for signal communication with the transmitter, the receiver of the monitoring equipment, or transceivers of the products;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of a chemical agent, a biological agent, a radiological agent, a nuclear agent, or an explosive agent which allows radio frequency (RF) data to be at least one of received or transmitted between the tag and the monitoring equipment.

16. A built-in, embedded multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents;

comprising a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor;

comprising a communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal for monitoring products, interconnected to a built-in sensor array or fixed detection device for communication therebetween;

wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan or signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;

wherein the built-in embedded multi-sensor detection device receives a signal via any of one or more products in any product grouping categories; and

wherein, when an alarm occurs, the built-in, embedded multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in a product groupings category of design similarity comprising at least one of product-to-product, product-to-satellite, product-to-cellular, product-to-long range radio frequency, product-to-short range radio frequency, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop for communication therebetween;

wherein the built-in embedded multi-sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of the several product groupings of design similarity.

17. A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:

a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor;

monitoring equipment of at least one of products grouped together by common features in a product groupings category of design similarity comprising at least one of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone for the receipt and transmission of signals therebetween;

wherein the built-in multi-sensor detection device is built in any of one or more products comprising a maritime cargo container, a lock, or the monitoring equipment;

wherein the built-in multi-sensor detection device is implemented by business or government by products grouped together by common features in at least one of several product groupings of design similarity;

a light alarm indicator that has a plurality of colored lights that correspond to specific agents of the at least two agents;

wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity comprising at least one of product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop for at least one of a receipt or transmission of signals therebetween.

18. A built-in multi sensor detection system for detecting at least two items selected from the group consisting of chemical agent, biological agent, radiological agent, explosive agent, human agent, contraband agent, motion, perimeter, temperature, tampering, theft, or breach, comprising:

a built-in sensor array or fixed detection device into a product that detects items by means of at least two sensors from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor;

monitoring equipment of at least one of the products grouped together by common features in a product groupings category of design similarity comprising at least one of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone for the receipt and transmission of signals therebetween;

wherein the built-in, multi-sensor detection device is built in any of one or more products comprising a maritime cargo container, a lock, or the monitoring equipment;

wherein, when an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in a product groupings category of design similarity comprising at least one of product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop for the receipt and transmission of signals therebetween;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of the chemical agent, the biological agent, the radiological agent, the explosive agent, the human agent, the contraband agent, the motion, the perimeter, the temperature, the tampering, the theft, and the breach which allows radio frequency (RF) data to be received and/or transferred between the tag and the monitoring equipment.

19. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, radiological agent, or compound, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human, or contraband agent or compound, capable of being disposed within, on, upon or adjacent a multi-sensor detection device;

monitoring equipment comprising at least one of a computer, personal computer (PC), laptop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone for at least one of a receipt or transmission of signals therebetween;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication between the multi-sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi-sensor detection device and the monitoring equipment;

whereupon a signal sent to a receiver of the multi-sensor detection device from a satellite; or to a cell phone tower; or through at least one of a short range radio frequency or a long range radio frequency; causes a signal to be sent to the monitoring equipment that includes at least one of location data or sensor data;

wherein the monitoring equipment or multi-sensor detection device receives a signal via any of one or more products of any product grouping categories;

wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency connection, or short range radio frequency (RF) connection is capable of signal communication with the transmitter, a receiver of the monitoring equipment, the multi-sensor detection device, or transceivers of the products;

wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan or signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;

wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, long range radio frequency, and short range radio frequency (RF).

20. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, radiological agents or compound, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human, or contraband agent or compound, capable of being disposed within, on, upon or adjacent a multi-sensor detection device;

monitoring equipment of at least one of products grouped together by common features in a product groupings category of design similarity comprising at least one of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA), or smart phone for at least one of a receipt or transmission of signals therebetween,

wherein the monitoring equipment is equipped with a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (to make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom; or at least one satellite capable of transmitting signals to the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication between the multi-sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi-sensor detection device and the monitoring equipment; and

whereupon a signal sent to a receiver of the multi-sensor detection device from a satellite; or to a cell phone tower; or through at least one of a short range radio frequency or a long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and/or sensor data;

wherein the multi-sensor detection device is implemented by business or government by products grouped together by common features in at least one of several product groupings of design similarity;

wherein the multi-sensor detection device is for any of one or more products comprising a maritime cargo container, a lock, or the monitoring equipment;

wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency connection, or short range radio frequency connection is in signal communication with a transmitter and a receiver of the monitoring equipment or multi-sensor detection device and transceivers of the products.

21. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human, or contraband agent or compound, capable of being disposed within, on, upon or adjacent a multi-sensor detection device, wherein at least one of the sensors is capable of detecting agents of an item of interest (IOI);

monitoring equipment of at least one of the products grouped together by common features in a product groupings category of design similarity comprising at least one of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA), or smart phone for at least one of a receipt or transmission of signals therebetween;

at least one satellite or at least one cell phone tower capable of signal communication between the multi-sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi-sensor detection device and the monitoring equipment;

whereupon a signal sent to a receiver of the multi-sensor detection device for detecting the agents of the item of interest causes a signal that includes at least one of location data or sensor data to be sent to the monitoring equipment;

wherein the multi-sensor detection device for any of one or more products comprising a maritime cargo container, a lock, or the monitoring equipment;

wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, or broadband connection, is in signal communication with a transmitter, a receiver of the monitoring equipment, or transceivers of the products;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of the explosive agent, the nuclear agent, the contraband agent, the chemical agent, the biological agent, the human agent, or the radiological agent which allows radio frequency (RF) data to be received and/or transferred between the tag and the monitoring equipment.

22. A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal, comprising:

at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;

a receiver for receiving signals, data or messages from at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long and/or short range radio frequency (RF) connection, or GPS connection;

the communication device being at least a fixed, portable or mobile communication device, equipped with at least one wired or wireless sensor for the detection of humans;

the communication device being equipped to receive signals from or send signals to engage (lock), disengage (unlock), or disable (make unavailable) locks;

the communication device being equipped with biometrics that incorporates at least one of a fingerprint recognition or a face recognition to at least one of gain access to the device or to prevent unauthorized use;

the communication device being capable of wireless near-field communication (NFC) which allows radio frequency (RF) data to be at least one of received or transferred between the communication device and at least one tag that is read by the communication device;

whereupon a signal sent to the receiver of at least one of a multi-sensor detection device, a cell phone detection device, or a locking device from a satellite or a cell phone tower or through at least one of a Bluetooth connection, a WiFi connection, an internet connection, a cellular connection, a GPS connection, a short range radio frequency (RF) connection, or a long range radio frequency (RF) connection, causes a signal that includes at least one of location data or sensor data to be sent to the communication device; and

wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection, capable of signal communication with the transmitter of the communication device, the receiver of the communication device, or the central processing unit (CPU).

23. A cell phone comprising:

a central processing unit (CPU) for executing and carrying out the instructions of a computer program;

a transmitter for transmitting signals and messages to a cell phone detection device;

a receiver for receiving signals from the cell phone detection device;

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;

the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and

whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;

at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;

wherein at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection is capable of signal communication with the transmitter or the receiver;

wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and

whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.

* * * * *

Exhibit C

US010163287B2

(12) **United States Patent**
Golden

(10) **Patent No.: US 10,163,287 B2**
(45) **Date of Patent: Dec. 25, 2018**

(54) **MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM**

(71) Applicant: **Larry Golden**, Greenville, SC (US)

(72) Inventor: **Larry Golden**, Greenville, SC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **15/530,839**

(22) Filed: **Mar. 6, 2017**

(65) **Prior Publication Data**

US 2017/0186259 A1 Jun. 29, 2017

Related U.S. Application Data

(60) Continuation of application No. 14/806,988, filed on Jul. 23, 2015, now Pat. No. 9,589,439, which is a continuation of application No. 14/021,693, filed on Sep. 9, 2013, now Pat. No. 9,096,189, which is a continuation of application No. 13/288,065, filed on Nov. 3, 2011, now Pat. No. 8,531,280, which is a

(Continued)

(51) **Int. Cl.**

G08B 27/00	(2006.01)
G07C 9/00	(2006.01)
B60R 25/24	(2013.01)
B60R 25/04	(2013.01)

(52) **U.S. Cl.**
CPC ***G07C 9/00174*** (2013.01); ***B60R 25/04*** (2013.01); ***B60R 25/24*** (2013.01); ***G07C 9/00007*** (2013.01); ***G07C 9/00563*** (2013.01)

(58) **Field of Classification Search**
CPC .. G07C 9/00; G07C 9/00007; G07C 9/00174; G07C 9/00309; G07C 9/00388; G07C 9/00563; G08B 27/00; G08B 27/005; G08B 27/006; B60R 25/018; B60R 25/04; B60R 25/10; B50R 25/102
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,385,469	A	5/1983	Scheuerpflug et al.
4,544,267	A	10/1985	Schiller

(Continued)

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and dated Jan. 13, 2012, pp. 1-34, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (34 pages).

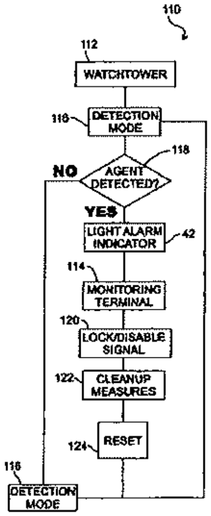
(Continued)

Primary Examiner — Van Trieu

(57) **ABSTRACT**

A multi sensor detection and disabling lock system includes detector cases for holding interchangeable detectors that sample for chemical, biological and radiological compounds, agents and elements, with each detector case disposed in or upon the monitored product. The detector case transmits detection information to a monitoring computer terminal and transmits a signal to a lock disabler engaged to the product to lock or disable the product's lock thereby preventing untrained, unauthorized and unequipped individuals from gaining access and entry to the product, and also preventing further contamination of the area. The detection system can be interconnected to surveillance towers scanning detector cases disposed at seaport docks, freight depots and rail terminals for monitoring containers being prepared for shipment or sitting on docks for long periods of time.

6 Claims, 13 Drawing Sheets



Related U.S. Application Data

division of application No. 12/802,001, filed on May 27, 2010, now Pat. No. 8,334,761, which is a continuation of application No. 12/657,356, filed on Jan. 20, 2010, now Pat. No. 8,106,752, which is a continuation of application No. 12/155,573, filed on Jun. 6, 2008, now Pat. No. 7,636,033, which is a continuation-in-part of application No. 11/397,118, filed on Apr. 5, 2006, now Pat. No. 7,385,497.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,586,441	A	5/1986	Zekich	
4,792,226	A	12/1988	Fishbine et al.	
5,222,152	A	6/1993	Fishbine et al.	
5,223,844	A	6/1993	Mansell et al.	
5,233,404	A	8/1993	Lougheed et al.	
5,557,254	A	9/1996	Johnson et al.	
5,682,133	A	10/1997	Johnson et al.	
5,766,956	A	6/1998	Groger et al.	
5,938,706	A	8/1999	Feldman	
5,959,529	A	9/1999	Kail	
5,963,657	A	10/1999	Bowker et al.	
5,986,543	A	11/1999	Johnson	
5,990,785	A	11/1999	Suda	
6,049,269	A	4/2000	Byrd et al.	
6,078,265	A	6/2000	Bonder et al.	
6,262,656	B1	7/2001	Byrd et al.	
6,271,745	B1	8/2001	Anzai et al.	
6,374,652	B1	4/2002	Hwang	
6,411,887	B1	6/2002	Martens et al.	
6,470,260	B2	10/2002	Martens et al.	
6,542,076	B1	4/2003	Joao	
6,542,077	B2	4/2003	Joao	
6,588,635	B2	7/2003	Vor Keller et al.	
6,610,977	B2	8/2003	Megerle	
6,613,571	B2	9/2003	Cordery et al.	
6,628,813	B2	9/2003	Scott et al.	
6,647,328	B2	10/2003	Walker	
6,738,697	B2	5/2004	Breed	
6,923,509	B1	8/2005	Barnett	
6,980,092	B2	12/2005	Turnbull et al.	
6,988,026	B2	1/2006	Breed et al.	
7,005,982	B1	2/2006	Frank	
7,034,677	B2	4/2006	Steinthal et al.	
7,034,683	B2	4/2006	Ghazarian	
7,103,460	B1	9/2006	Breed	
7,116,798	B1	10/2006	Chawla	
7,148,484	B2	12/2006	Craig et al.	
7,171,312	B2	1/2007	Steinthal et al.	
7,184,117	B2	1/2007	Breed et al.	
7,243,945	B2	7/2007	Breed et al.	
7,339,469	B2	3/2008	Braun	
7,346,439	B2	3/2008	Bodin	
7,350,608	B2 *	4/2008	Fernandez	B60L 1/00 180/65.1
7,385,497	B2	6/2008	Golden	
7,397,363	B2	7/2008	Joao	
7,636,033	B2	12/2009	Golden	
7,647,180	B2	1/2010	Breed	
7,844,505	B1	11/2010	Arneson et al.	
7,868,912	B2	1/2011	Venetianer et al.	
7,872,575	B2	1/2011	Tabe	
7,880,767	B2	2/2011	Chinigo	
7,961,094	B2	6/2011	Breed	
8,120,459	B2 *	2/2012	Kwak	G07C 9/00309 340/5.2
8,274,377	B2	9/2012	Smith et al.	
8,531,521	B2	9/2013	Romanowich	
8,564,661	B2	10/2013	Lipton et al.	
2002/0145666	A1	10/2002	Scaman	
2003/0063004	A1	4/2003	Anthony et al.	
2003/0137426	A1	7/2003	Anthony et al.	
2003/0179073	A1 *	9/2003	Ghazarian	E05B 47/00 340/5.6
2003/0206102	A1	11/2003	Joao	
2004/0107028	A1	6/2004	Catalano	
2004/0222092	A1	11/2004	Musho	
2005/0195069	A1	9/2005	Dunand	
2006/0164239	A1	7/2006	Loda	
2006/0176169	A1	8/2006	Doolin et al.	
2006/0181413	A1	8/2006	Mostov	
2006/0250235	A1	11/2006	Astrin	
2007/0093200	A1 *	4/2007	Dobosz	H04B 7/18565 455/3.02
2007/0171042	A1	7/2007	Metes et al.	
2007/0257774	A1 *	11/2007	Stumpert	G06Q 10/08 340/7.1
2008/0045156	A1	2/2008	Sakhpara	
2008/0122595	A1	5/2008	Yamamichi et al.	
2008/0234907	A1	9/2008	Labuhn et al.	
2010/0159983	A1	5/2010	Golden	
2011/0178655	A1	6/2011	Golden	

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and dated Dec. 2, 2011, pp. 1-27, publisher United States and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (27 pages).

United States Patent and Trademark Office; Office Action, Office Action from U.S. Appl. No. 13/065,837; copyright and dated Nov. 1, 2011, pp. 1-18, publisher United States Patent and Trademark Office, Alexandria, Virgina, USA; U.S. Appl. No. 13/288,065 (18 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 11/397,118; dated Nov. 14, 2007; Alexandria, Virgina, USA; pp. 1-12; U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; dated Apr. 9, 2009; Alexandria, Virgina, USA; pp. 1-7; U.S. Appl. No. 13/288,065 (7 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; dated Jul. 30, 2009; Alexandria, Virgina, USA; pp. 1-9; U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/155,573; dated Oct. 28, 2009; Alexandria, Virgina, USA; pp. 1-5; U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/657,356; dated Jul. 12, 2010; Alexandria, Virgina, USA; pp. 1-14; U.S. Appl. No. 13/288,065 (14 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/657,356; dated Mar. 10, 2011; Alexandria, Virginia, USA; pp. 1-4; U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 13/065,837; dated Jul. 18, 2011; Alexandria, Virgina, USA, pp. 1-9; U.S. Appl. No. 13/288,065 (9 pages).

A newspaper article of Mr. Melvin Sullivan and his family that references the date, Mar. 5, 2001, U.S. Appl. No. 13/288,065.

A letter of response Mr. Sullivan received from Pfeiffer & Gantt, PA, dated Sep. 16, 2002, U.S. Appl. No. 13/288,065.

A "Certificate of Existance" Bright Idea Inventor, LLC. Nov. 6, 2002, U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Congressman from Maryland, Elijah E. Cummings, dated Dec. 16, 2002; U.S. Appl. No. 13/288,065.

A newspaper article of Mr. Melvin Sullivan and Mr. Larry Golden, dated Feb. 27-Mar. 5, 2003; U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated May 21, 2003; U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Office of the Vice President, Dick Cheney, dated Jun. 3, 2003; U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated Oct. 1, 2003; U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Lindsey O. Graham, dated Oct. 21, 2003; U.S. Appl. No. 13/288,065.

(56) **References Cited**

OTHER PUBLICATIONS

A letter sent to the President of the United States George W Bush, the President's Cabinet, the United States Senate and the Congressional Black Caucus, dated May 23, 2005; U.S. Appl. No. 13/288,065.

On Nov. 17, 2005, an "Inventor's Office Record of Invention", was filed in my name (Golden) at "The Law Office of David P. Gaudio,P.C.; the Inventors Network."; U.S. Appl. No. 13/288,065.

On Aug. 23, 2005, the "Disclosure Document Registration"; U.S. Appl. No. 13/288,065.

On Apr. 5, 2006, the "Patent Application" was filed in my name (Golden) at the United Staets Patent & Trademark Office in Washington, D.C.; U.S. Appl. No. 13/288,065.

On Jun. 6, 2008, the "Continuance-In-Part, (CIP) Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; U.S. Appl. No. 13/288,065.

On Jan. 20, 2010, a "Continuation Application" (U.S. Appl. No. 12/657,356) was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033,"Swear Back"; in accordance to Title 37—Code of Federal Regulations Patents, Trademarks, and Copyrights; Apr. 8, 2011; U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033; "Swearback-History of Work"; Apr. 8, 2011; U.S. Appl. No. 13/288,065.

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001, dated Apr. 14, 2011, 2011; Alexandria, Virginia, USA; pp. 1-16; U.S. Appl. No. 13/288,065 (16 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; dated May 27, 2011; Alexandria, Virginia, USA; pp. 1-14, U.S. Appl. No. 13/288,065 (14 pages).

United States Department of Homeland Security: Petition for Inter Partes Review of U.S. Pat. No. Re. 43,990 Under 35 U.S.C. §312 and 37 C.F.R. §42.104; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA: pp. 1-57; U.S. Appl. No. 14/806,988 (57 pages).

United States Department of Homeland Security; Declaration of Dr. Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington D.C., USA; pp. 1-44; U.S. Appl. No. 14/806,988 (44 pages).

Richard R Brooks and S.S. Iyengar; Multi-Sensor Fusion Fundamentals and Applications with Software; published 1998; Copyright Prentice Hall PTR; Upper Saddle River, New Jersey, USA; pp. 1-20; copy enclosed (20 pages), U.S. Appl. No. 14/806,988 (20 pages).

Ramanarayanan Viswanathan and Pramod K Varshney; Distriubted Detection with Multiple Sensors: Part I—Fundamentals; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-11; vol. 85; No. 1; Southern Illinois University Carbondale OpenSIUC: Illinois. USA; pp. 1-11; U.S. Appl. No. 14/806,988 (11 pages).

Blum; Distributed Detection with Multiple Sensors: Part II—Advanced Topics: Proceedings of the IEEE; Jan. 1, 1997; pp. 1-16; vol. 85, No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; U.S. Appl. No. 14/806,988 (16 pages).

Victor Lesser; Distributed Sensor Networks a Multiagent Perspective; 2003; pp. 1, 2, 5, 6322, 26, 27, 36, 275, 320: copyright 2003 Kluwer Academic Publishers; AH Dordrecht, The Netherlands; U.S. Appl. No. 14/806,988 (10 pages).

Samuel Blackman and Robert Popoli; Design and Analysis of Modern Tracking Systems; 1999; pp. 1, 2, 6, 472; copyright 1999 Artech House; Norwood, Massachusetts, USA; U.S. Appl. No. 14/806,988 (4 pages).

Jean-Francois Chamberland; Decentralized Detection in Sensor Networks; 2003; pp. 407-416 IEEE Transactions on Signal Processing; vol. 51, No. 2; Urbana, Illinois, USA; U.S. Appl. No. 14/806,988 (10 pages).

Oleg Kachirski and Ratan Guha; Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks; pp. 1-8; Proceedings of the 36.sup.th Hawaii International Conference on System Sciences; copyright 2003; Orlando, Florida. USA; U.S. Appl. No. 14/806,988 (8 pages).

Lawrence A Klein; Sensor and Data Fusion a Tool for Information Assessment and Decision Making; 2004; pp. 1-4, 6, 81, 87-89; copyright 2004 The Society of Photo-Optical Instrumentation Engineers; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Waehington, USA; U.S. Appl. No. 14/806,988.

Dale Ferriere and Khrystyna Pysareva and Andrzej Rucinski; Using Technology to Bridge Maritime Security Gaps; Aug. 1, 2005; Sea Technology; pp. 1-6; copyright Compass Publications, Inc. Jan. 2009; Portsmouth, New Hampshire. USA; U.S. Appl. No. 14/806,988 (6 pages).

Corie Lok; Cargo Security; MIT Technology Review; Jun. 2004; No. 107; pp. 74-75; publisher is Massachusetts institute of Technology; Cambridge, Massachusetts, USA; USPASN14/806988 (2 pages).

Thomas C Chen; RFID and Sensor-based Container Content Visibility and Seaport Security Monitoring system; Proceedings of SPIE, vol. 5778; pp. 151-159; Mar. 28, 2005; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; USPASN14/806988 (10 pages).

United States Department of Homeland Security; The University of Texas at Austin College of Engineering Standard Resume of Sriram Vishwanath; CaseIPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr, 30, 2014; Washington, D.C., USA; pp. 1-21; USPASN14/806988 (21 pages).

Operating Agreement of Bright Idea Inventor, LLC received from Pfeiffer & Gantt, PA, dated Nov. 13, 2002; U.S. Appl. No. 13/288,065.

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; dated Oct. 20, 2011; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages); U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and dated Dec. 12, 2011, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA, parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and dated Mar. 26, 2012, pp. 1-12, publisher United States Patent and Trademark Office; Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and dated Feb. 22, 2012, pp. 1-38, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (38 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and dated Feb. 22, 2012, pp. 1-25, publisher United States Patent and Trademark office, Alexandria, Virginia, USA, U.S. Appl. No. 13/288,065 (25 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and dated Aug. 24, 2012, pp. 1-4, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and dated Nov. 28, 2012, pp. 1-11, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (11 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and dated Apr. 16, 2013, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virgina, USA; U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and dated Apr. 20, 2015, pp. 1-20, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 14/021,693 (20 pages).

United States Patent and Trademark Office, Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and dated Jan.

(56) **References Cited**

OTHER PUBLICATIONS

20, 2015, pp. 1-17, publisher United States Patent and Trademark Office, Alexandria, Virgina, USA; U.S. Appl. No. 14/021,693 (17 pages).
United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and dated Sep. 5, 2014, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 14/021,693 (12 pages).
United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/806,988; copyright and dated Jul. 5, 2015, pp. 1-5, publisher United States Patent and Trademark Office, Alexandria, Virgina, USA; parent U.S. Appl. No. 14/806,988 (5 pages).
United States Patent and Trademark Office; Notice of Allowance from U.S. Appl. No. 14/806,988; dated Jan. 3, 2017; Alexandria, Virgina, USA; pp. 1-8; U.S. Appl. No. 14/806,988 (8 pages).
United States Patent and Trademark Office; Notice of Allowaance from U.S. Appl. No. 14/021,693; dated Jun. 19, 2015; Alexandria, Virginia, USA; pp. 1-8; U.S. Appl. No. 14/021,693 (8 pages).
United States Patent and Trademark Office; Notice of Allowaance from U.S. Appl. No. 13/288,065; dated May 24, 2013; Alexandria, Virgina, USA; pp. 1-8; U.S. Appl. No. 13/288,065 (8 pages).

* cited by examiner

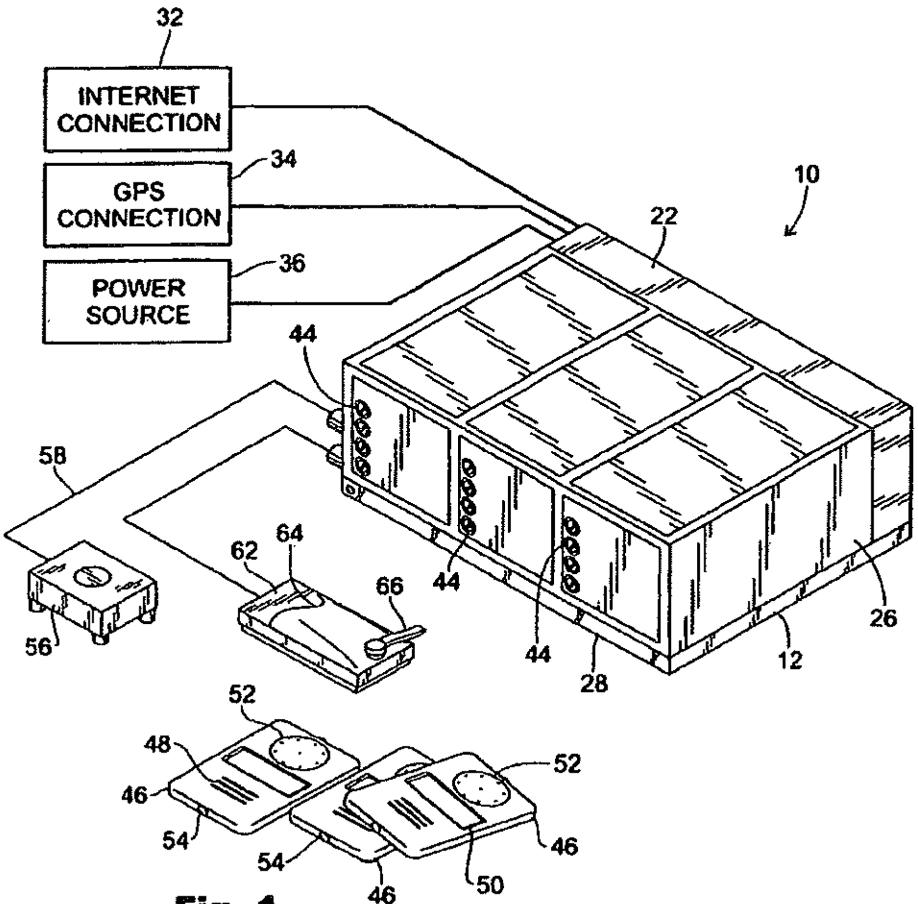

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
44
58
62
64
66
44
44
26
12
28
56
52
48
46
54
54
46
52
46
50

Fig. 1

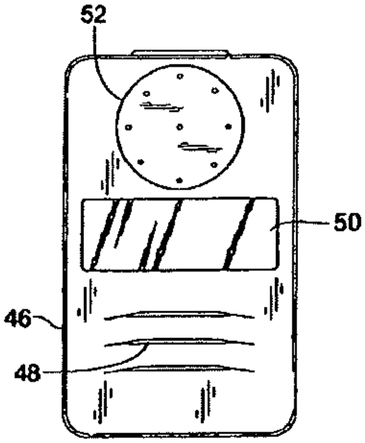

52
50
46
48

Fig. 2

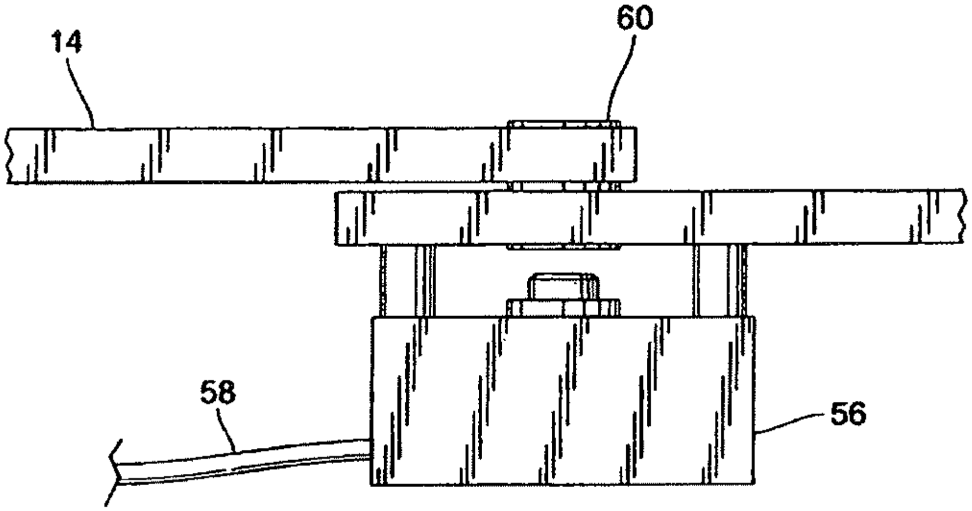


Fig. 3a

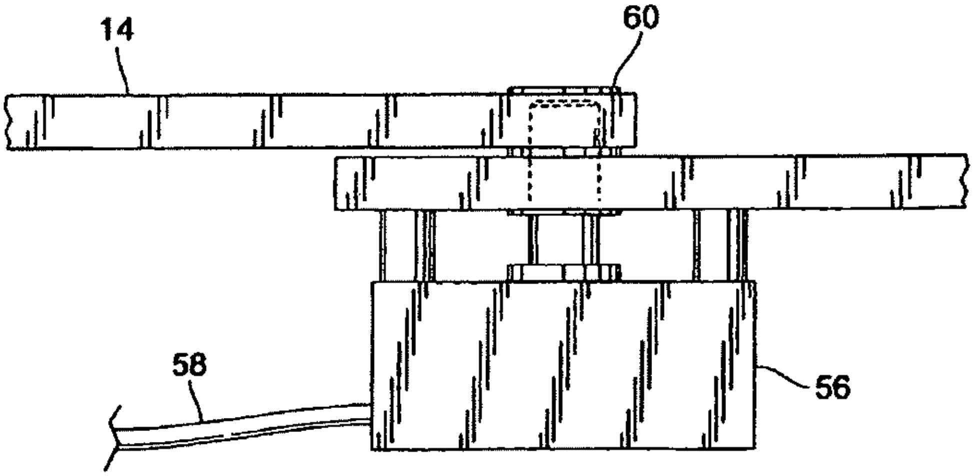


Fig. 3b

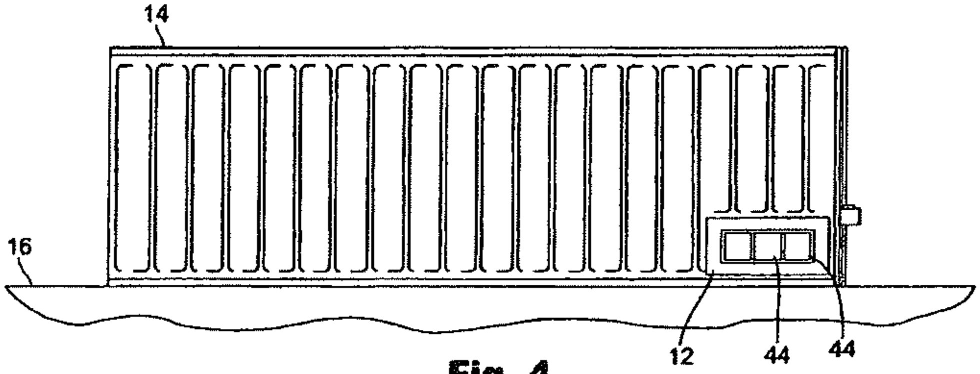


Fig. 4

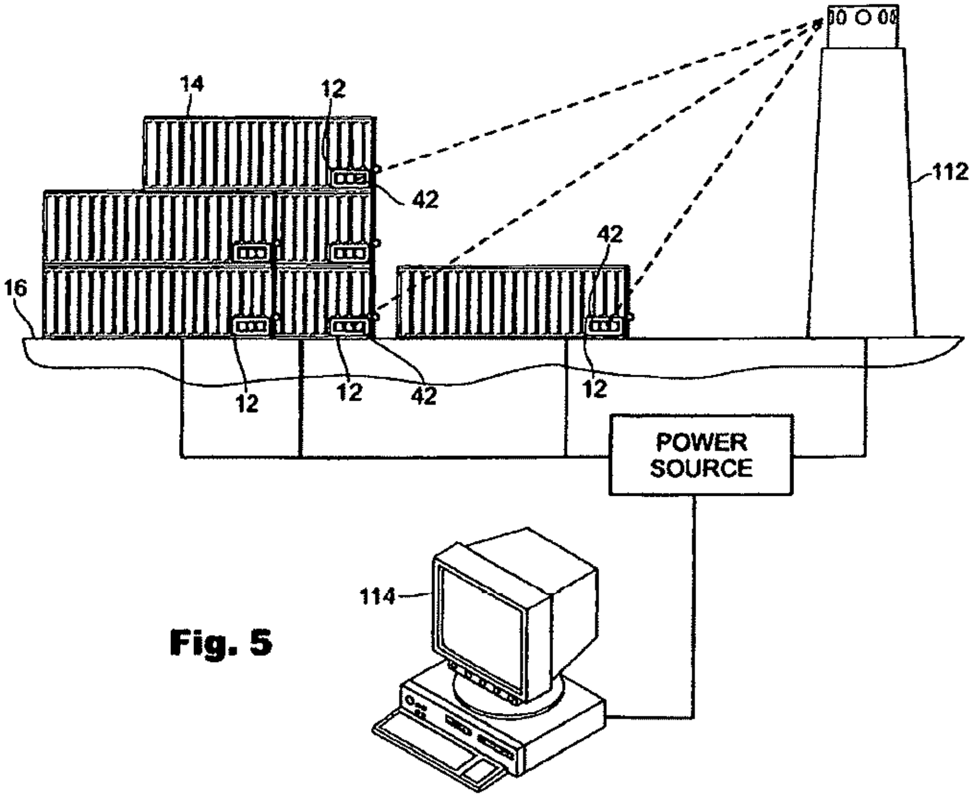


Fig. 5

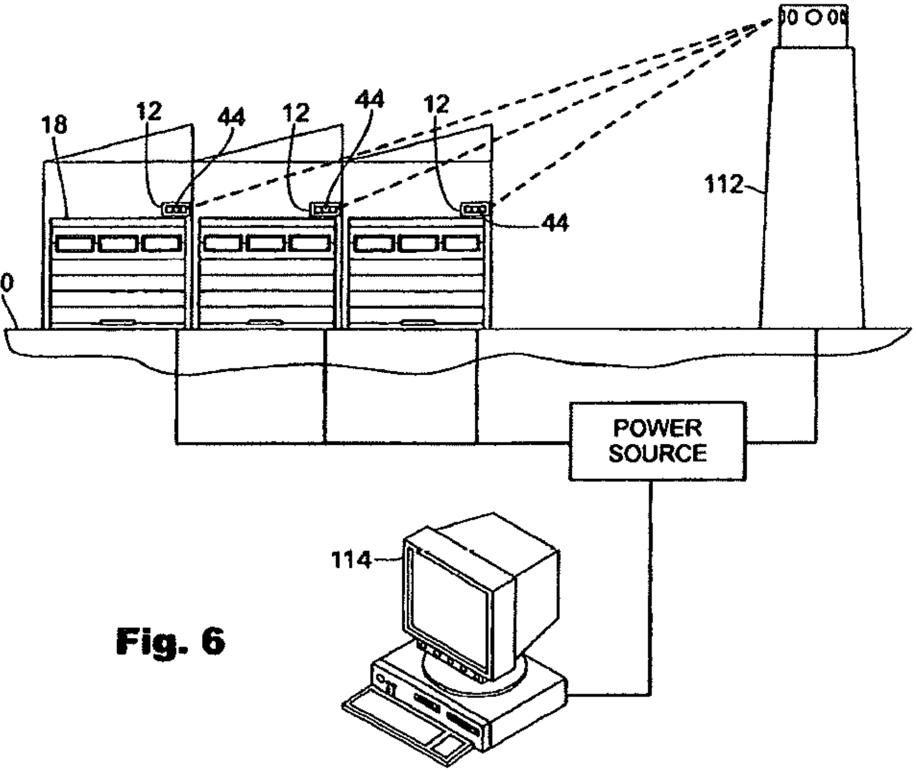


Fig. 6

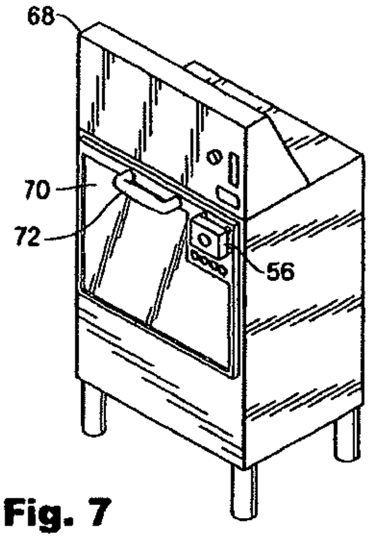


Fig. 7

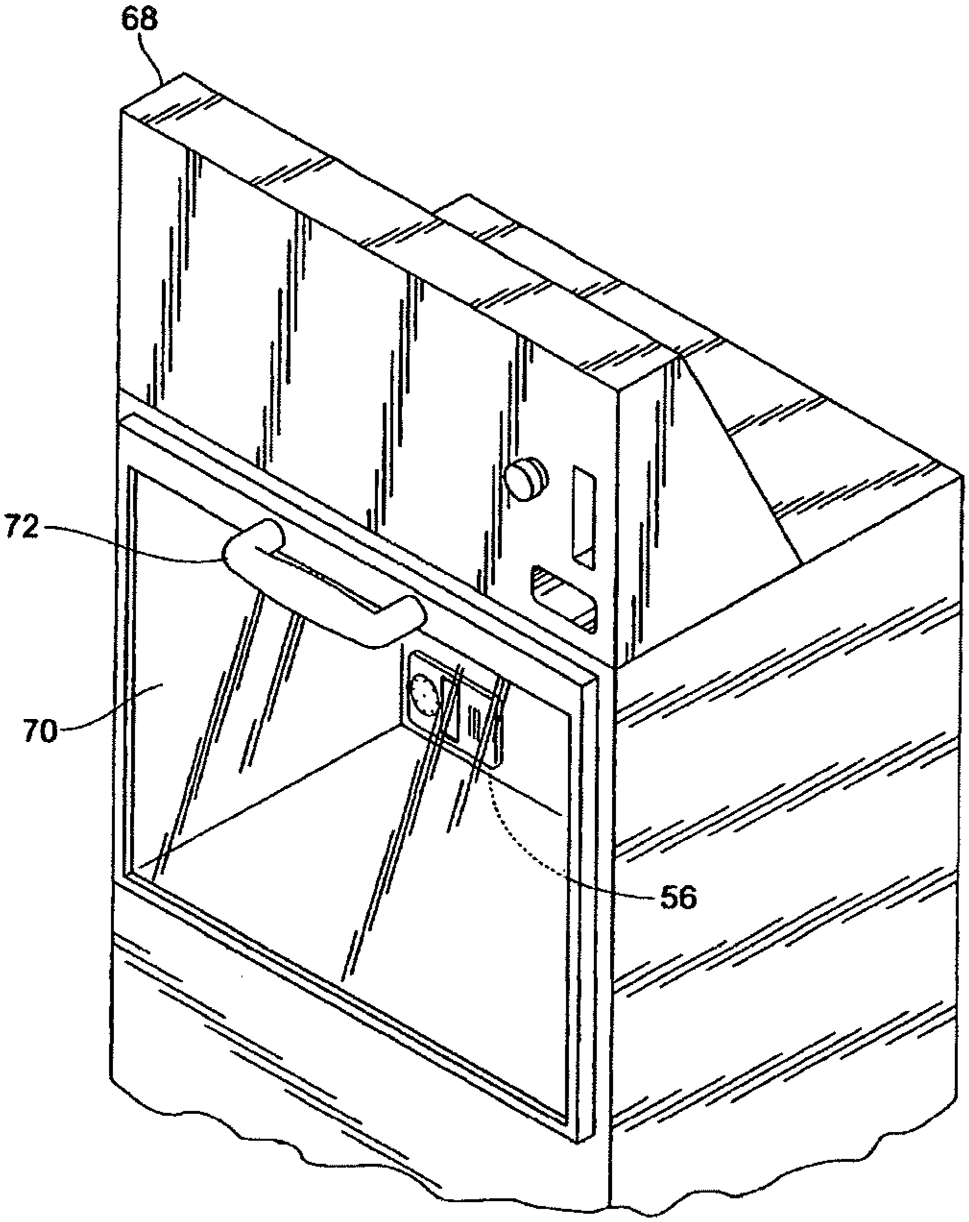


Fig. 8

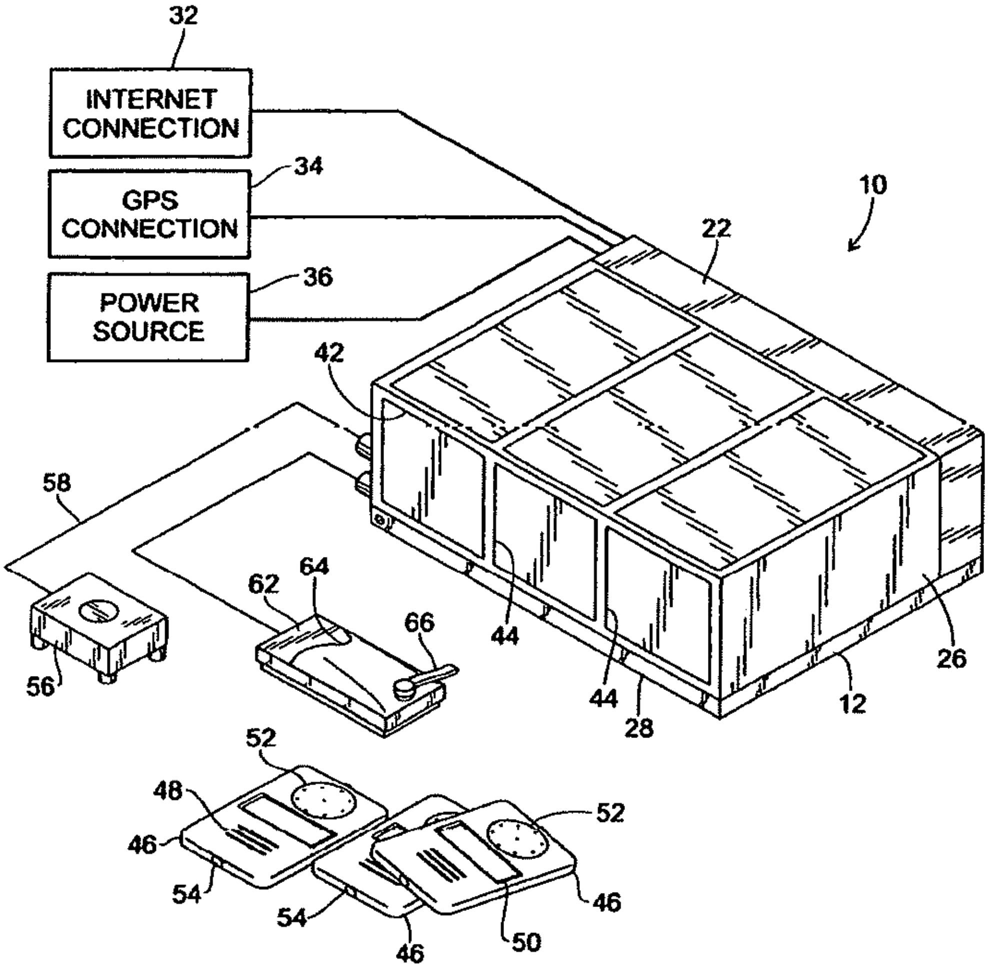

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
42
58
64
62
66
44
44
28
12
26
56
52
48
46
54
54
46
50
52
46

Fig. 9

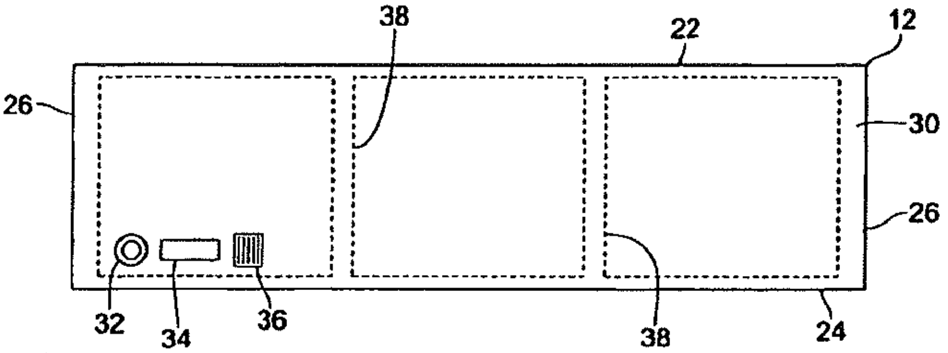

38
22
12
26
30
26
32
34
36
38
24

Fig. 10

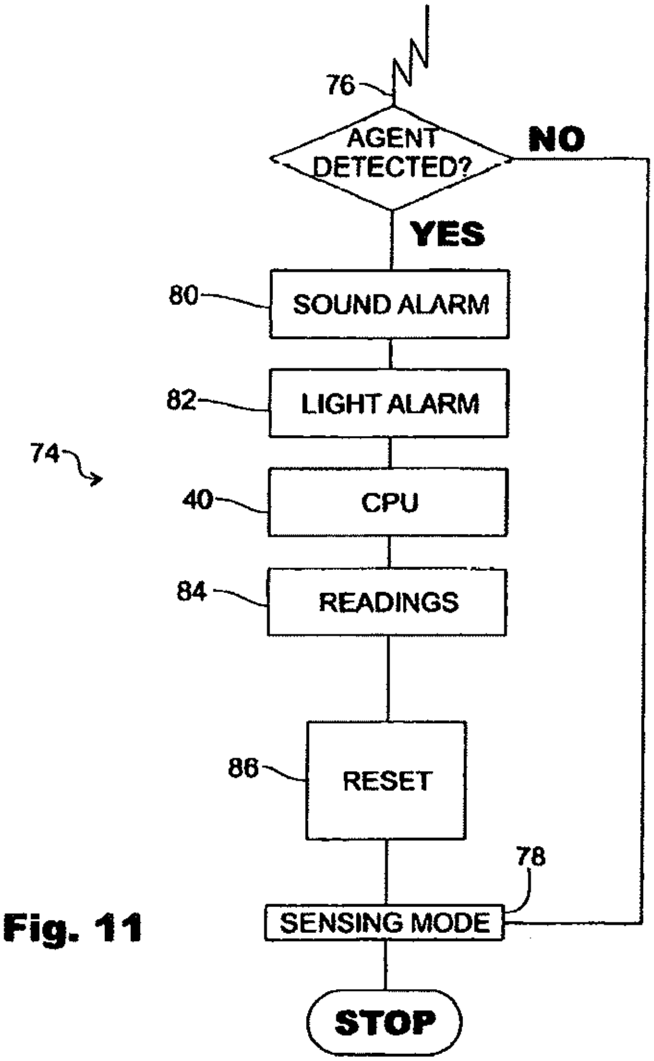

76
AGENT DETECTED?
NO
YES
80
SOUND ALARM
82
LIGHT ALARM
74
40
CPU
84
READINGS
86
RESET
78
SENSING MODE
STOP

Fig. 11

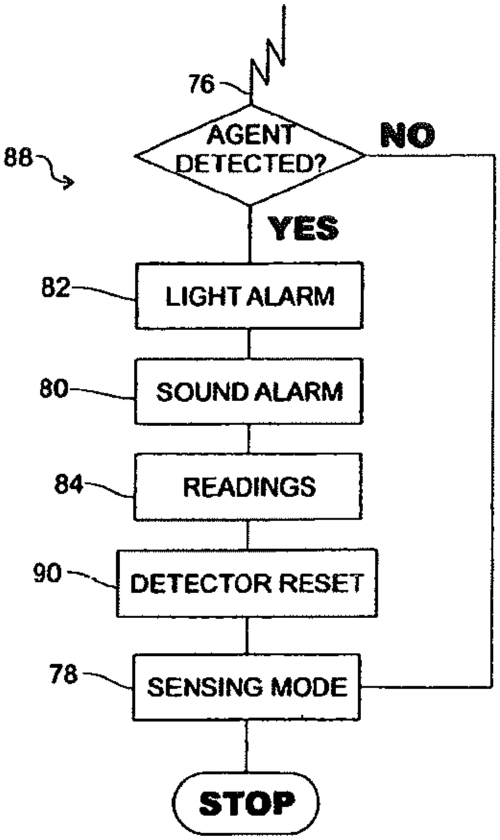

76
AGENT DETECTED?
NO
88
YES
82
LIGHT ALARM
80
SOUND ALARM
84
READINGS
90
DETECTOR RESET
78
SENSING MODE
STOP

Fig. 12

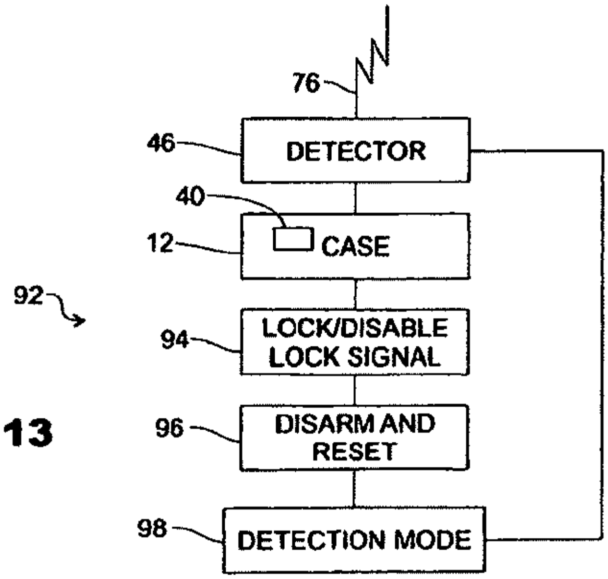

76
46
DETECTOR
40
12
CASE
92
94
LOCK/DISABLE LOCK SIGNAL
96
DISARM AND RESET
98
DETECTION MODE

Fig. 13

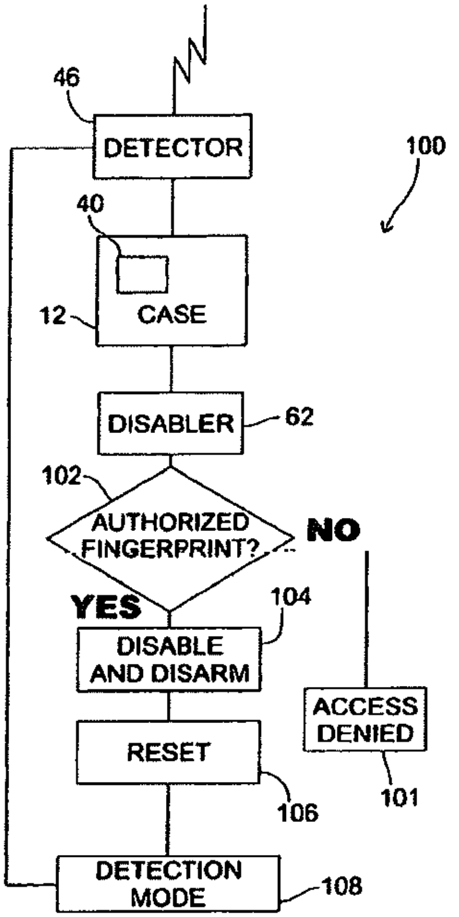

46
DETECTOR
100
40
12
CASE
DISABLER
62
102
AUTHORIZED FINGERPRINT?
NO
YES
104
DISABLE AND DISARM
ACCESS DENIED
RESET
106
101
DETECTION MODE
108

Fig. 14

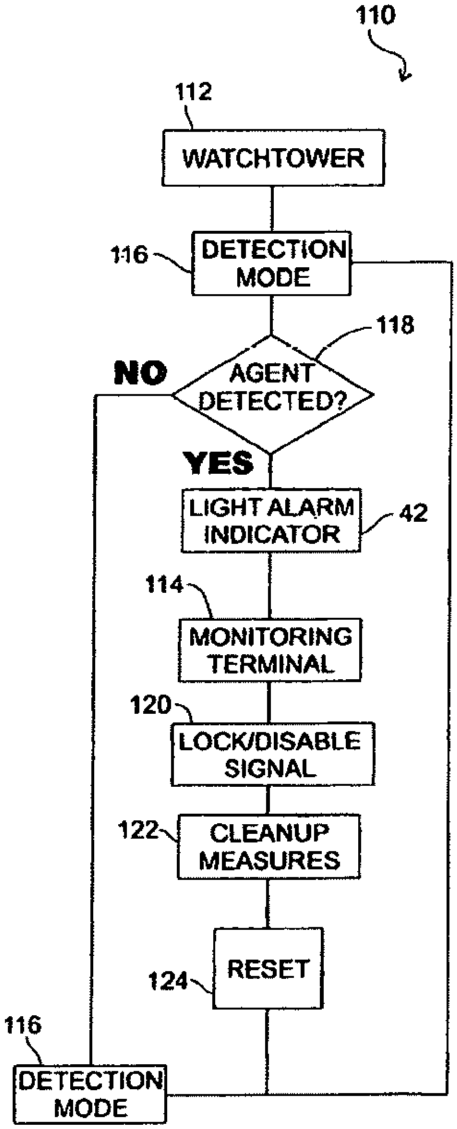

110
112
WATCHTOWER
116
DETECTION MODE
118
NO
AGENT DETECTED?
YES
LIGHT ALARM INDICATOR
42
114
MONITORING TERMINAL
120
LOCK/DISABLE SIGNAL
122
CLEANUP MEASURES
124
RESET
116
DETECTION MODE

Fig. 15

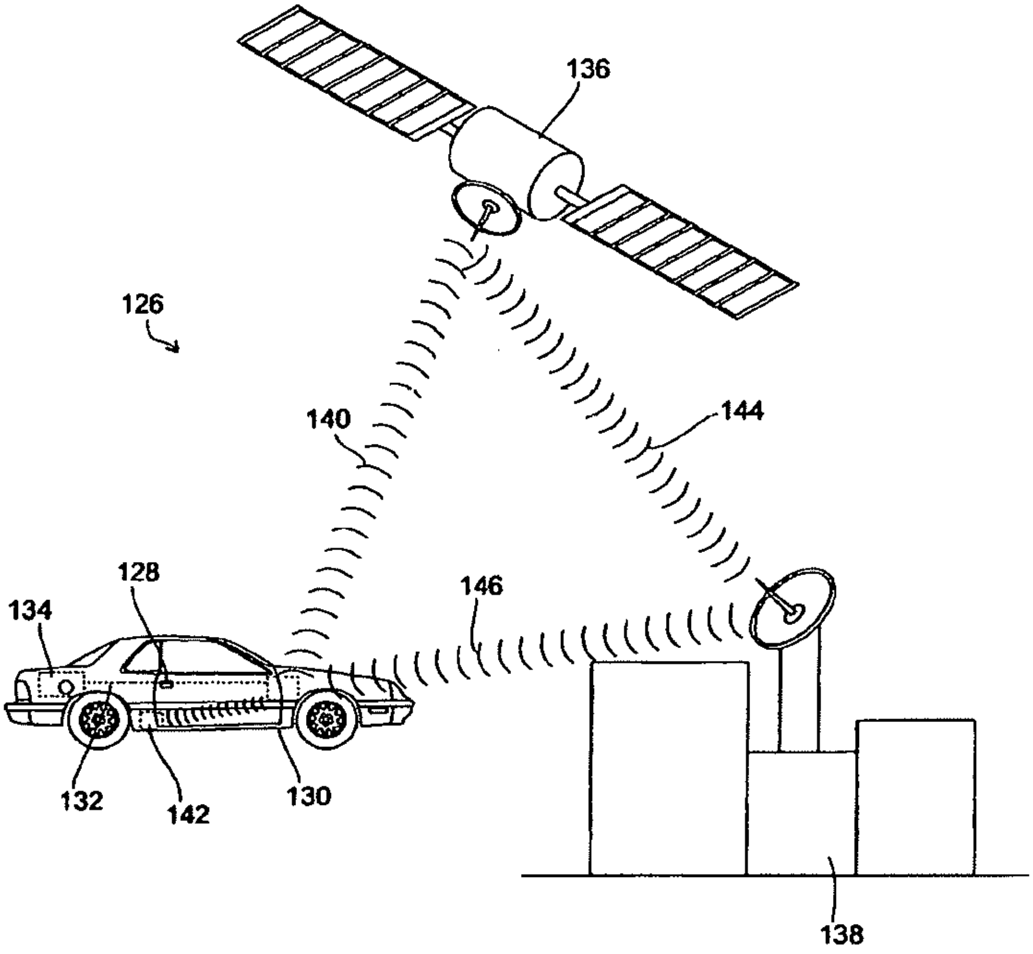


Fig. 16

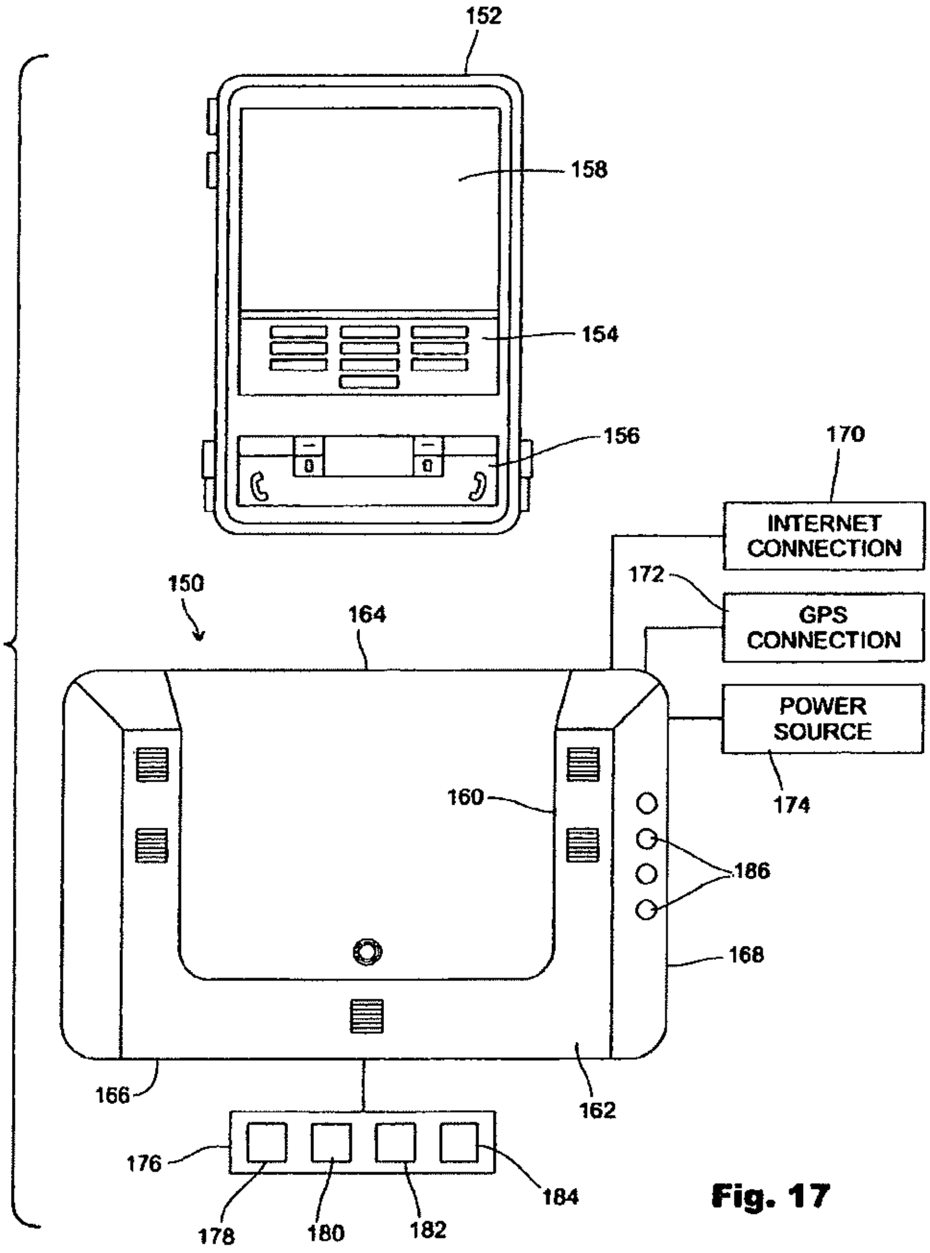

152
158
154
156
170
INTERNET CONNECTION
172
GPS CONNECTION
POWER SOURCE
174
150
164
160
186
168
166
162
176
178
180
182
184

Fig. 17

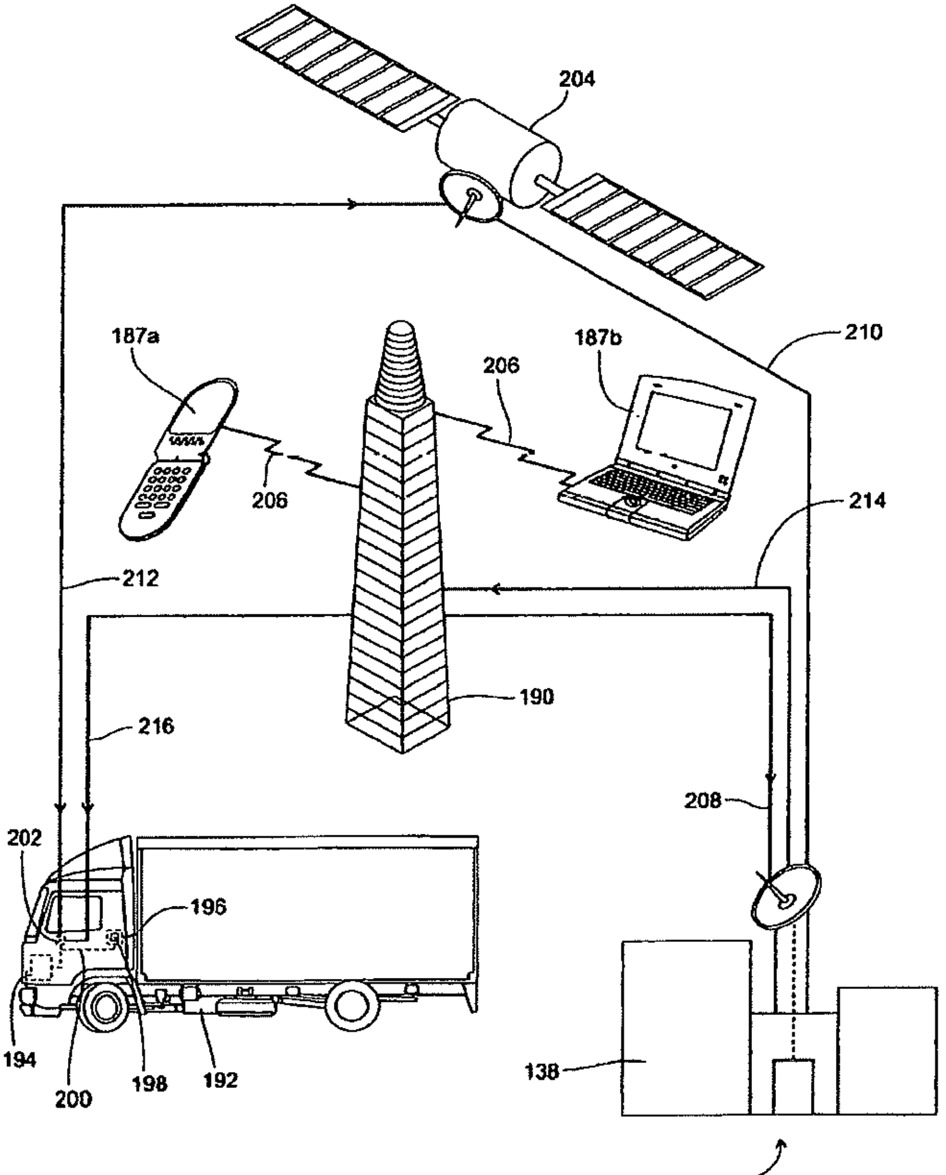

204
187a
206
187b
210
206
214
212
190
216
208
202
196
194
200
198
192
138
188

Fig. 18

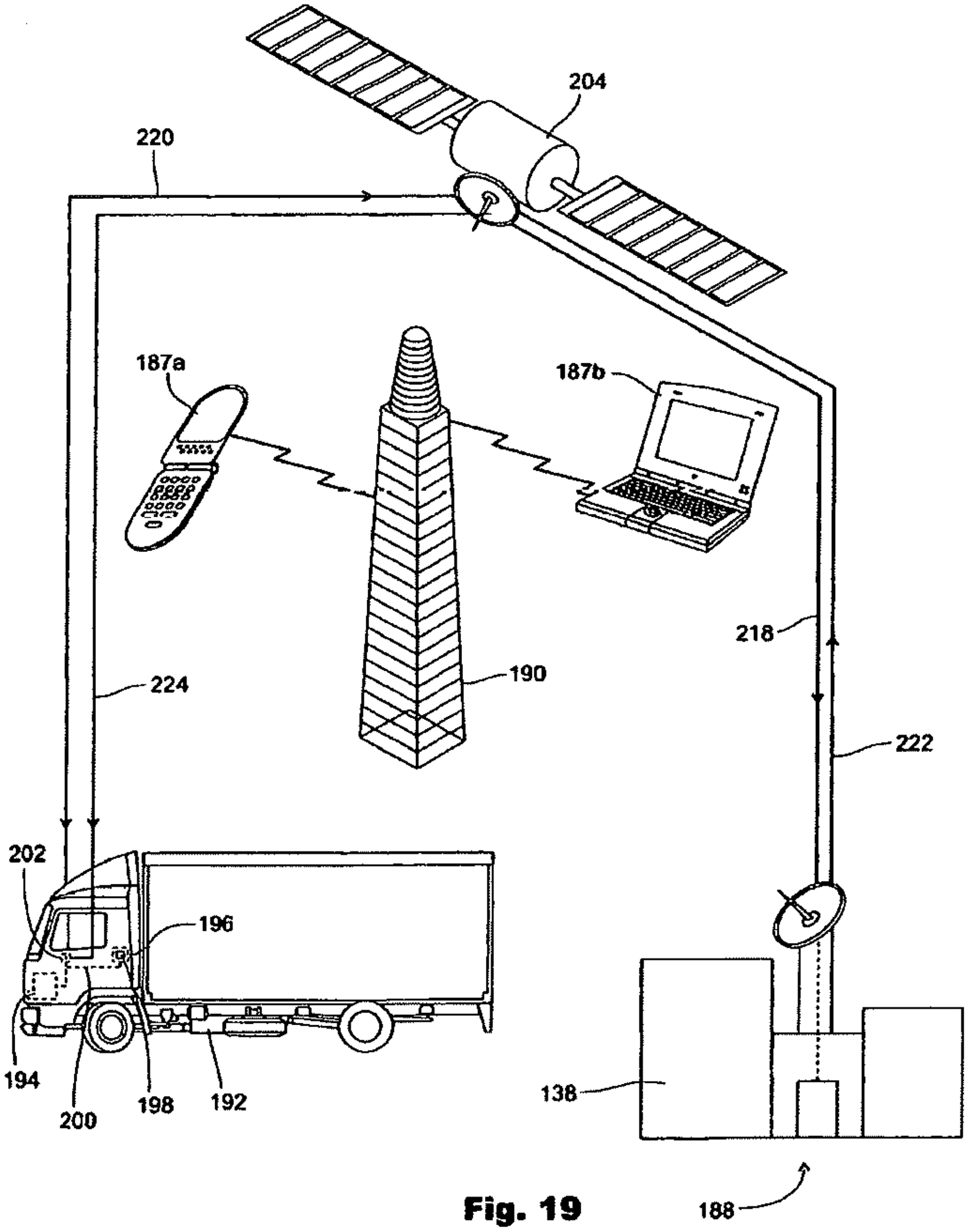

204
220
187a
187b
218
224
190
222
202
196
194
200
198
192
138
188

Fig. 19

MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM

CROSS REFERENCE TO RELATED APPLICATION

This application is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 14/806,988 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Jul. 23, 2015 that issued on Mar. 7, 2017 as U.S. Pat. No. 9,589,439, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 9,589,439 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 14/021,693 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Sep. 9, 2013 that issued on Aug. 4, 2015 as U.S. Pat. No. 9,096,189, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 9,096,189 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 13/288,065 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Nov. 3, 2011 that issued on Sep. 10, 2013 as U.S. Pat. No. 8,531,280, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 13/288,065 that will issue as U.S. Pat. No. 8,531,280 is a divisional application and claims the filing date and benefit of U.S. patent application Ser. No. 12/802,001 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on May 27, 2010, that issued on Dec. 18, 2012 as U.S. Pat. No. 8,334,761, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 8,334,761 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 12/657,356 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Jan. 20, 2010 that issued on Jan. 31, 2012 as U.S. Pat. No. 8,106,752 the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 8,106,752 is a continuation of and claims priority to U.S. Pat. No. 7,636,033. U.S. Pat. No. 7,636,033 is a continuation-in-part of and claims priority to U.S. Pat. No. 7,385,497. U.S. patent application Ser. No. 13/288,065 that will issue as U.S. Pat. No. 8,531,280 also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/657,356, now U.S. Pat. No. 8,106,752 herein by reference for all purposes. The present application also claims the filing date and benefit of and incorporates the entire contents of U.S. Pat. Nos. 9,096,189; 8,531,280; 8,334,761; 8,106,752; 7,636,033; and 7,385,497 by reference herein in their entireties for all purposes.

FIELD OF THE INVENTION

The present invention pertains to anti-terrorist detection and prevention systems, and more particularly pertains to a disabling lock mechanism combined with a chemical/biological/radiological detection system for use with products grouped together by similar characteristics in order to prevent unauthorized entry, contamination and terrorist activity.

BACKGROUND

Terrorist activity is a continuous, daily, worldwide threat to the stability, prosperity, security and peace within nations and between and among nations. Its danger lies in its arbitrary destructiveness as much as in its unpredictability, and the constant threat of terrorist activity compels measures and actions that cause strain and contention in free, democratic societies as security concerns and civil liberty concerns must be balanced so that both public safety and civil liberties are maintained. Safety and security concerns can be addressed through numerous proactive steps and measures, many of which cause only minimal interference with and disruption of the daily routines of work, travel, commerce and entertainment. However, because modern industrial societies afford almost limitless places, locations, and opportunities for terrorist activities, no safety measure or security protocol will be foolproof, but many security measures, systems and protocols can be implemented that greatly minimize specific threats through fingerprint identification procedures, chemical, biological, and radiological hazard detections, bomb and explosive detection, and controlling the access to everything from shipping containers to school lockers. Thus, the prior art discloses a wide range of security measures and systems.

For example, the Fishbine et al. patent (U.S. Pat. No. 4,792,226) discloses an optical fingerprinting system that includes an optics/processor unit, a video monitor, a data terminal, and a printer for collecting and storing data characteristics of all ten individual fingerprints for printing demographic information and fingerprint images as desired on a standard booking or applicant card.

The Schiller patent (U.S. Pat. No. 4,544,267) discloses a finger identification unit that includes a fingerprint scanning apparatus using a collimated beam of light to interrogate the fingerprint of a finger placed against a platen so that successive scan positions produce signals containing fingerprint information.

The Fishbine et al. patent (U.S. Pat. No. 5,222,152) discloses a portable fingerprint scanning apparatus for optically scanning and recording fingerprint images and wirelessly transmitting such images to a mobile processing unit for verification and background checking.

The Lougheed et al. patent (U.S. Pat. No. 5,233,404) discloses an optical scanning apparatus that uses a linear charge coupled device (CCD) for recording the image of a fingerprint on the viewing surface.

The Groger et al. patent (U.S. Pat. No. 5,766,956) discloses a diode laser based sensor for undertaking optical, chemical, immunological or nucleic acid-based assay or other chemical analysis.

The Feldman patent (U.S. Pat. No. 5,938,706) discloses a multi element security system for preventing the unauthorized use of an automotive vehicle, and which includes numerous locking and control features interconnected to an onboard cpu.

The Bowker et al. patent (U.S. Pat. No. 5,963,657) discloses a safety access control for doors, handles, locks, etc., wherein the surface relief of a finger is read and verified to either allow or prevent access by the individual to the door, handle, lock, etc.

The Bonder et al. patent (U.S. Pat. No. 6,078,265) discloses a fingerprint identification security system wherein a key lock operated security system utilizes the fingerprint of the individual to control user access to the security system, such as the ignition system of an automotive vehicle.

The Anzai et al. patent (U.S. Pat. No. 6,271,745 B1) discloses a keyless authorization system for use of a motor vehicle that includes fingerprint reading units located on the exterior or interior of the motor vehicle and which are coupled to a control unit for scanning, comparing and matching fingerprints to allow or disallow access to the motor vehicle.

The Hwang patent (U.S. Pat. No. 6,374,652 B1) discloses a fingerprint-activated doorknob in which a detecting sensor for a fingerprint is placed on the doorknob for measuring and searching the fingerprint against previously stored fingerprint inputs to control access to the door.

The Vor Keller et al. patent (U.S. Pat. No. 6,588,635 B2) discloses a safety holster for a firearm that includes a pivotally mounted retaining member and a fingerprint sensor for scanning fingerprint information so that only authorized users can withdraw the firearm from the holster.

The Cordery et al. patent (U.S. Pat. No. 6,613,571 B2) discloses a method and system for detecting biological and chemical hazards in the mail that includes sensors placed within the mail box for sampling and testing ambient air and so that mail can be safely transported through the mail system.

The Nagata patent (U.S. Pat. No. 6,628,213 B2) discloses a coding method for digital signal coding and decoding that includes a CMI (code-marked inversion) method of signal coding.

Nonetheless, despite the ingenuity of the above devices, methods, and systems, there remains a need for a multi-detector and disabling lock system for use with various types of products collected together by common characteristics into product groupings for detecting chemical, biological and radiological agents and compounds and for selectively disabling and activating the product locks thereby preventing unauthorized entry and further contamination and preventing and thwarting terrorist activities.

SUMMARY

The present invention comprehends a chemical/biological/radiological detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes and lockers; while the products grouped into what may be referred to as Product grouping 2 include, but are not limited to, chemical, biological, radiological, and nuclear detectors, motion sensors and door sensors. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The multi sensor detection and lock disabling system includes a detector case sized to fit in, upon or adjacent any of the aforedescribed products for detecting harmful and dangerous chemical, biological, and radiological agents, compounds and elements. In addition, the multi sensor detection and lock disabling system is capable of transmitting a signal to lock or disable a lock on the product, and is also capable of transmitting signals to a monitoring computer terminal or PC so that appropriate defensive and safeguarding actions can be undertaken and an authorized individual can disarm and reset the locking system and the multi sensor detection system. The detector case includes a power source (battery or electrical), interior compartments, Internet and GPS connections and a cpu interconnected with the Internet and GPS connections, and also interconnected with one or more off site monitoring computer terminals or PCs. The detector case includes one or more light alarm indicators that are externally visible and that light up when the chemical, biological, or radiological agent or compound is detected, and the light alarm indicators (which can be indicator lights or panels on the front of the detector case) can be color coded for denoting the specific agent or compound detected, i.e., separate and distinct colors for indicating detection of the chemical, biological, or radiological agent or compound.

The detector case is designed to hold within the interior compartments one or more interchangeable detectors, and each detector is adapted and set up to sample a specific compound or agent. Each detector includes a sound alarm, a sensor, a light alarm, and a readings panel, and is electrically interconnected (either by wire or wirelessly) to the cpu of the detector case so that information regarding the detection of the particular agent or compound can be conveyed from the detectors to the detector case cpu. Each detector can also be used as a manual, stand-alone hand held scanner.

The multi sensor detection and lock disabling system can be interconnected to a surveillance watchtower, as well as monitoring computer terminals or PCs, with the watchtower scanning shipping and cargo crates and containers being prepared for shipment or sitting for extended periods of time on a dock or at a port, at a railway site, or at an industrial storage facility. The watchtower will scan the cargo and shipping crates and containers for the light alarm indicators on detector cases that are mounted in or upon the crates and containers, and thus continuous security surveillance of the crates and containers can be maintained.

An enhanced version of the multi sensor detection and lock disabling system can be employed to prevent car and vehicle bombings. Coupling the multi sensor detection and lock disabling system with satellite service will enable the detection system to detect explosives and transmit an alert signal by satellite to monitoring equipment at a monitoring site. Upon receiving the alert signal at the monitoring site the monitoring equipment activates a stall-to-stop process for disabling the air, fuel, electrical and/or computer system of the vehicle. Moreover, upon receiving the alert signal at the monitoring site the car or vehicle will be locked by transmission of a satellite signal that disables the vehicle's electrical and ignition system thereby preventing escape of the terrorist.

It is an objective of the present invention to provide a multi sensor detection and disabling lock system for securing news racks and vending machines in order to prevent theft, unauthorized use and terrorist activity.

It is another objective of the present invention to provide a multi sensor detection and disabling lock system for preventing terrorist activity by using products grouped together by common features in several product groupings such as design similarity, similarity in the presentation of security problems and similarity with regard to the presentation of solutions to preventing terrorist solutions.

It is still yet another objective of the present invention to provide a multi sensor detection and disabling lock system that is capable of disabling an existing lock or activating a lock inside any of the products of the product grouping lists when a detector or sensor of the system is activated.

It is still yet a further objective of the present invention to provide a multi sensor detection and disabling lock system wherein the disabling lock system prevents the unauthorized entry, access and further contamination of the products included in the several product groupings.

A still further objective of the present invention is to provide a multi sensor detection and lock disabling system that utilizes a multi-task device for preventing terrorist activity to vulnerable products that are collected or arranged by product grouping categories.

Yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system to secure cargos and containers, especially cargo and shipping containers, against chemical, biological, radiological and nuclear terrorist activity.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system capable of detecting chemical, biological and radiological agents and compounds.

Still yet another objective of the present invention is to provide a multi sensor detection and disabling lock system that includes interchangeable detectors that operate in conjunction to detect chemical, biological and radiological agents and compounds.

Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories.

Another objective of the present invention is to provide a multi sensor detection and disabling lock system that accurately and reliably detects harmful agents, compounds and elements, and prevents the placement and storage of weapons and bombs in the range of storage containers and facilities currently available.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system wherein the interchangeable detectors that comprise part of the system can be used as stand-alone scanners.

These and other objects, features, and advantages will become apparent to those skilled in the art upon a perusal of the following detailed description read in conjunction with the accompanying drawing figures and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the primary features of the system which include a detector case, several interchangeable detectors, an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler;

FIG. **2** is a front elevational view of the multi sensor detection and lock disabling system of the present invention illustrating one of the interchangeable detectors first shown in FIG. **1**;

FIG. **3***a* is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one lock disabler to the lock of a product, such as a container, and disengaged from the lock of the container;

FIG. **3***b* is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the engagement of the lock disabler to the lock of the product for locking or disabling the lock of the product so that unauthorized access is prevented;

FIG. **4** is a side elevational view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case mounted to the product, such as the container, with the light alarm indicators externally visible;

FIG. **5** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of detector cases with a surveillance watchtower and a monitoring PC terminal;

FIG. **6** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the placement of detector cases upon containers different from the containers of FIG. **5**, and wherein the detectors case are interconnected to a surveillance watchtower and a monitoring PC terminal;

FIG. **7** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one automatic/mechanical lock disabler to the lock of a standalone news rack;

FIG. **8** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating one interchangeable detector placed within the standalone news rack;

FIG. **9** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case having color coded front panels for specifically indicating the agents, compounds or elements that have been detected;

FIG. **10** is a rear elevational view of the multi sensor detection and lock disabling system of the present invention illustrating the GPS, Internet and power source connections;

FIG. **11** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector with the detector case and the steps undertaken by the system when an agent or compound is detected;

FIG. **12** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the sequence of steps undertaken by one detector when functioning as a stand alone scanner for detecting an agent or compound;

FIG. **13** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector case with the automatic/mechanical lock disabler for activating the lock disabler upon detection by the system of an agent or compound;

FIG. **14** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating interconnection of the detector case with the fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public upon detection of the agent or compound;

FIG. **15** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the system with a surveillance watchtower and a monitoring PC or computer terminal for monitoring containers, such as shipping or cargo containers, that may sit for extended time periods on docks, at rail yards, and at industrial storage facilities;

FIG. **16** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the integration of the detection system with a satellite and monitoring equipment at a monitoring site for detecting explosives placed in a vehicle and then transmitting signals to the satellite and then to the monitoring site for disabling and locking the vehicle;

FIG. **17** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the features and elements of the detector case to a cell phone and cell phone case;

FIG. **18** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of a GPS satellite, a monitoring site and a cell phone tower for communicating to and with an electronic device such as a laptop computer or a cell phone for transmitting signals to a vehicle for activating an onboard stall-to-stop device for bringing the vehicle to a halt; and

FIG. **19** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the use of a GPS satellite in conjunction with the monitoring site and monitoring equipment to relay commands and signals to the cpu or transceiver of the vehicle for stopping or locking the vehicle in response to a signal that a certain type of event (detection of a bomb, engine failure or malfunction or unauthorized use) has occurred or is in process.

DETAILED DESCRIPTION OF REPRESENTATIVE EMBODIMENTS

Illustrated in FIGS. **1-19** is a multi sensor detection and lock disabling system **10** for preventing terrorist activity by monitoring, detecting, and securing those critical areas; sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities that are vulnerable to terrorist activity as convenient places to store and plant explosives and bombs and spread biological, chemical or radiological agents and compounds, followed by the disposition of the multi sensor detection and lock disabling system **10** for monitoring, detecting, and securing the particular location or site. Vulnerable sites, locations, facilities and areas are nearly limitless in their variety; in order to categorize the protection the present invention provides an anti-terrorist product grouping strategy has been developed wherein products made from the same or similar material, products having the same or similar design, and products presenting the same or similar security problems are grouped together with the multi sensor detection and lock disabling system **10** for preventing terrorist activity. For example, two preferred product groupings can be Product Grouping I: cargo containers, shipping containers, cargo planes, freight train cars, tractor trailers, mail carriers (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans and utility vehicles. Product Grouping II: chemical detectors, biological detectors, radiological detectors, nuclear detectors, motion sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems. In addition to grouping products together by features, designs and materials, the multi sensor detection system **10** includes a lock disabling capability for disabling an existing lock or activating a lock on or inside any of the aforementioned products when a detector or sensor of the system is activated. The lock disabling feature is a crucial component of the invention in so far as it prevents unauthorized, unequipped or untrained individuals from gaining access and entry to the site and causing further contamination of the site.

As shown in FIGS. **1-10**, the multi sensor detection and lock disabling system **10** includes at least one—and preferably many—detector case **12** that can be placed in, on, upon or adjacent the product, such as the shipping containers **14** of FIGS. **4** and **5** resting upon a platform **16** or the cargo container **18** of FIG. **6** sitting upon a seaport dock or pier **20**. The detector case **12** includes a top **22**, a bottom **24**, a pair of opposed sides **26** and a front side or panel **28** and an opposite rear or back side **30**. The rear side **30** has connections or contacts that can include an Internet connection **32**, a GPS connection **34** and a power connection **36** for a power source. The power source for the detector system **10** can be any conventional battery or electrical source. The detector case **12** includes an interior chamber divided into a number of compartments **38** for holding therein agent or compound detection means hereinafter further described. A cpu **40** is mounted within the detector case **12** and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment. The front side **28** of the detector case **12** includes indicator means for visually indicating that a specific agent, compound or element has been detected. The indicator means can include color coded indicator lights **42** in panel form, as shown in FIG. **9**, with each indicator light panel **42** lighting up with a specific color corresponding to the detection of a specific agent or compound; or color coded indicator lights **44**, as shown FIG. **1**, that correspond to and individually light up on the detection of a specific agent or compound (chemical, biological, or radiological).

As shown in FIGS. **1**, **2** and **9-13**, the multi sensor detection and lock disabling system **10** includes a plurality of detectors **46** with each detector **46** adapted for and set up to sample for a specific agent or compound (biological, chemical, or radiological); and the detectors **46** are interchangeable for adapting to the needs and demands of future technology. The detectors **46** can also be used as stand alone scanners. In the preferred embodiment of the invention, at least three detectors **46** are placed within the detector case **12** with one detector **46** for specifically sampling biological agents or compounds, one detector **46** for sampling chemical agents or compounds, and one detector **46** for sampling radiological agents or compounds. The detectors **46** are interconnected to the cpu **40** of the detection system **10** by conventional connections that can be wire or wireless for transmitting the appropriate signals to the cpu **40** upon detection of the particular agent or compound. As shown in FIG. **2**, each detector **46** includes on its front plate or facing surface a sound alarm indicator **48**, a readings panel **50** comprising a plastic shield and LED lights for displaying the various read-out messages, a sensor **52** for detecting the specific agent, element or compound, and a light alarm indicator **54** that can be color coded for each specific agent and which is externally visible when the detector **46** is used as a stand alone scanner. Each detector **46** includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the cpu **40** of the detector case **12**.

As shown in FIGS. **1**, **3*a***, **3*b***, **9**, and **13-15**, used in conjunction with the multi sensor detection and lock disabling system **10** is at least one automatic/mechanical lock disabler **56**—and depending upon the number of products being monitored there can be one lock disabler **56** for each product. The automatic/mechanical lock disabler **56** is physically connected to the detector case **12** by a wire or cable **58** for receiving signals therefrom for disabling an existing lock or activating a lock inside a product to prevent access to the product. By way of example, FIG. 3*a* shows the automatic/mechanical lock disabler **56** mounted—by any conventional means—to the lock **60** of the shipping container **14** shown in FIGS. **4** and **5** and connected by wire **58** to the cpu **40** of the detector case **12**. The lock disabler **56** is in the non-activated or disengaged state in FIG. 3*a*. FIG. 3*b* shows the automatic/mechanical lock disabler **56** mounted to the lock **60** of the shipping container **14** and in the activated or engaged state after detection of an agent or compound by the system **10** thereby for locking or disabling the lock **60** of the shipping container **14** and preventing unauthorized entry and access by unauthorized, untrained and unequipped individuals. In FIGS. 3*a* and 3*b* the lock **60** secures doors of the shipping container **14** that can be slidably or pivotably opened and closed.

In addition to the automatic/mechanical lock disabler **56**, the multi sensor detection and lock disabling system **10** can also utilize a fingerprint biometric lock with disabler **62** as shown in FIGS. **1** and **14**. The fingerprint biometric lock with disabler **62** is interconnected to the cpu **40** of the detector case **12** for receiving transmissions therefrom after detection of an agent or compound has occurred so that the lock on the product can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler **62** occurs when the fingerprint of the individual is placed on the fingerprint-matching pad **64**, and if a match occurs with a known fingerprint stored by the cpu **40**, then the individual can reset the fingerprint biometric lock with disabler **56** by turning the manual lock disabler **66**. The fingerprint biometric lock with disabler **62** is mounted to the lock of the product in a manner similar to the mounting of the automatic/mechanical lock disabler **56** that is shown in FIGS. **3** and 3*b*.

FIGS. **4** and **5** show one manner of disposition or placement of the detector case **12** in relation to the product, i.e., the shipping container **14**, with the color coded indicator lights **42** externally viewable; FIG. **5** shows a number of shipping containers **14** each equipped with a detector case **12** and integrated with elements hereinafter further described for continuously monitoring the shipping containers **14** as they sit for an extended period of time on the truck or rail platform **16**. FIG. **6** illustrates several cargo containers **18** sitting on the shipping dock or pier **20**, with each cargo container **18** having a detector case **12** mounted thereon and integrated with and monitored by elements shown in FIG. **5** and hereinafter further described.

FIG. **7** illustrates a typical product from product grouping 1 that is monitored by the multi sensor detection and lock disabling system **10** of the present invention; specifically, FIG. **7** shows a news rack **68** with one automatic/mechanical lock disabler **56** mounted to and interconnected with the locking mechanism of the news rack **68**. As long as there is no detection of any agent or compound, the lock disabler **56** is in the disengaged state, and the individual can deposit the coin amount in the chute and then freely open the glass panel **70** by the handle **72** for removing a paper. However, the lock disabler **56** would be activated upon detection of the harmful agent or compound and receipt of a signal from the cpu **40** for locking or disabling the locking mechanism thereby denying access to the interior of the news rack **68** from all untrained, unauthorized and unequipped individuals.

FIG. **8** illustrates one detector **46** disposed within the news rack **68** and which is visible through the panel **70** for detecting one specific agent, compound or element. The detector **46** functions as a stand-alone scanner and can be wirelessly interconnected to off site monitoring equipment.

FIG. **11** illustrates a representative schematic **74** for describing the signal transmission process from the detector **46** to the cpu **40** of the detector case **12**. The external stimulus **76** would be the chemical, biological or radiological agent or compound. If there is no detection of the agent or compound, the detector **46** will stay in the sensing mode **78**. However, detection of the specific agent will trigger the sound alarm **80** and the light alarm **82**, and instant transmittal of a signal to the cpu **40**. The readings **84** can be stored by the cpu **40** for verification and future review and evaluation. After all the appropriate corrective and preventative measures have been undertaken by the trained and authorized personal, and the site has been cleansed of the contamination, authorized and equipped personal can then reset **86** the system **10**.

FIG. **12** illustrates a representative schematic **88** for the detector **46** when used as stand-alone scanner. The detector **46** undergoes the same essential steps as illustrated in FIG. **11**, with the exception of the signal transmission to the cpu **40**. The detector **46** remains in detection mode **78** until an agent is detected, and then the various functions-light alarm **82**, sound alarm **80**, storage of readings **84**, and, after the appropriate security and safety steps have been carried out by authorized personal, detector reset **90** by authorized personal can occur thereby placing the detector **46** back in detection or sensing mode **78**.

FIG. **13** is a representative schematic **92** that illustrates the steps undertaken by the system **10** to lock or disable a lock, such as the lock **60** for the shipping container **14** shown in FIGS. 3*a* and 3*b*. Upon detection of the agent (chemical, biological, radiological) the alarm light indicators **42** or **44** will light up providing external indication that an agent has been detected. In addition, the system **10**—the cpu **40**—will transmit a lock/disable lock signal **94** to the automatic/mechanical lock disabler **56** to lock or disable the lock on the product, such as the lock **60** on the shipping container **14** of FIGS. 3*a*-**5**. This prevents unauthorized, unequipped, or untrained individuals from entering or gaining access to the product for which a dangerous and perhaps lethal agent has been detected. After the proper authorities and authorized personal have been notified and all the appropriate security, preventative and clean up measures have been undertaken, the authorized individual can perform the disarm and reset function **96** for the system **10** placing the system **10** in back in the detection mode **98**.

FIG. **14** is a representative schematic **100** illustrating the use of the fingerprint biometric lock with disabler **62** with the system **10**. Upon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the cpu **40** would then transmit a signal to the fingerprint biometric lock with disabler **62** to lock or disable the lock on the product, such as the lock **60** on the shipping containers **14** shown in FIGS. 3*a*-**5**. The shipping containers **60** would remain locked and in an access denied mode **101** should an attempt be made to gain access to the container **60** by opening the lock **60** with an unauthorized fingerprint. However, a fingerprint that matches stored and authorized fingerprints **102** would indicate an authorized individual, and would allow the individual to disable and disarm **104** the lock **60** of the shipping container **14**. The fingerprint biometric lock with disabler **62** would then be reset **106** after the appropriate safety, cleanup, and protection measures are completed, and the system **10** would be reset and placed back in the detection mode **108**.

FIG. **15** is a schematic representation **110** that illustrates the integration of a surveillance watchtower **112** and a monitoring terminal or PC **114** for monitoring products such as the shipping containers **14** or cargo containers **16** that sit for extended periods of time of docks, piers **20**, truck terminals, rail yards, shipping platforms **16** and industrial sites as shown in FIGS. **5** and **6**. The watchtower **112** would maintain continuous surveillance over a number of shipping containers **60**, for example, with detector cases **12** mounted in or on each container **14** and set in detection mode **116** with one or more detectors **46** disposed in each detector case **12**. The watchtower **112** would continuously scan for light alarm indicators **42** and **44** on the products, such as the containers **14** or **18**, and the watchtower **112** would be interconnected and integrated with the monitoring terminal or PC **114**. Upon detection **118** of an agent or compound in one or more of the shipping containers **14**, the appropriate light alarm indicators **42** or **44** would light providing visible confirmation of the detection of the specific agent or compound. The cpu **40** would transmit a lock/disable signal **120** to the lock **60** on each respective shipping container **14** to lock or disable the lock **60** thus preventing access to that respective shipping container **14**. In addition, signal transmissions would be sent to the monitoring terminal or PC **114** (which could be off site) thereby alerting authorized security personal of the contamination event. With the information received at the monitoring terminal **114**, authorized personal would then be notified and dispatched to the area to undertake the appropriate safety and cleanup measures **122**. Such measures would also include disarming the lock disabling system in order to gain access to the shipping container **14**. After all the cleanup and security measures are completed by the trained and properly equipped authorities, the detection system and the lock disabling feature would reset **124** and the detection system would again be placed in detection mode **116**.

FIG. **16** is a schematic representation **126** that illustrates an enhanced version of the multi sensor detection and lock disabling system **10** for preventing car and vehicle attacks and bombings. The lock disabling system **10** would be interconnected to the locking system and mechanism **128** of the vehicle **130**. In addition, a stall to stop disabling link **132** can be made with the fuel, air, and electrical system **134** of the vehicle **130**. The enhanced version incorporates a satellite **136** for signal receipt and transmission from the vehicle **130** in which the detector system **10** is placed to a monitoring site and monitoring equipment **138**. As shown in FIG. **16**, a detection signal **140** would be sent to the satellite **136** by the detection system **10** upon detection of a bomb or explosive **142** hidden in the vehicle **130**. The satellite **136** would then transmit an alert signal **144** to the monitoring site **138** with the signal **144** containing the relevant data to evaluate the nature of the threat. The monitoring site **138** would then transmit a stall to stop signal **146** to the detection system **10** to lock the vehicle **130** and/or disable the electrical system of the vehicle **130** thereby disabling the vehicle **130**, preventing access to the vehicle **130** by locking the vehicle **130**, and preventing any terrorist in the vehicle **130** from escaping.

The detector case **12** can be modified and adapted for inclusion with cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases; and briefcases. In addition, the basic monitoring terminal or PC **114**, as shown in FIGS. **5** and **15**, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring.

The system **10** and the watchtower **112**, along with the satellite **136** and the monitoring site **138** can be adapted or incorporated with cell phone towers and satellites for use with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu **40**, or a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween. The aforementioned telecommunication and radio communication means can be interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships and airplanes, and which is reported stolen, experiences a loss of brakes, or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted to the vehicle and which detection causes an automatic signal transmission or a signal transmission is activated when a call is made to the monitoring station by an authorized person. The authorized individual includes but is not limited to the owner, pilot, conductor, captain, police highway patrol, security guard and military personnel to the monitoring equipment for activating a vehicle slowdown or stall-to-stop disabling system that similar to the disabling system **126** shown in FIG. **16**, or incorporating features of the system **126** shown in FIG. **16**, from the monitoring equipment to the vehicle. The activation of the stall-to-stop disabling means or the vehicle slowdown disables or engages the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.

In addition, the basic stall-to-stop disabling means or the vehicle slowdown means and device can be adapted, modified or designed to include: an open bust or open platform for integrating any new and innovative technology; warning lights indicators; sound alarm indicators; voice alarm indicators; a cell phone to transmit to the vehicle a signal for slowing and halting the vehicle; and a lock disabling system or means to lock a thief or terrorist inside the vehicle after a transmission is received or sent. Open bust or open platform also refers to the compatibility of the detector case **12**, or the incorporation of its features in cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, briefcases, and suitcases, etc., with other communication, transmission and surveillance systems whereupon the detector case **12**, and its features, can be seamlessly integrated with other new and emerging systems and technologies.

Thus, as shown more specifically in FIG. **17**, by way of a representative example the features and elements of the detector case **12** are shown as being incorporated into cell phone detector case **150** and associated cell phone monitor **152**. The cell phone monitor **152** includes the standard keypad functions **154** and more specialized system use (ring tone, email, photos, texting) functions **156** as well as a viewing screen **158**. The cell phone detector case **150** includes a recharging cradle or seat **160**, a front side **162**, a top **164**, a bottom **166**, and a pair of opposed sides **168**. At the back of the cell phone detector case **150** are connections, contacts, and ports for at least an Internet connection **170**, a GPS connection **172**, and a contact, plug, or port for a power source **174**. The power source for the cell phone detector case **150** can be any conventional rechargeable battery source or standard electrical power from a standard electrical receptacle or outlet.

As shown in FIG. **17**, the cell phone detector case **150** includes one or more sensor/detector units, cells, or components 176 built into and incorporated into the case 150. The detector 176 includes generally disposed at the front 162 of the case 150 the following types of indicators: a sound alarm indicator 178, a readings panel 180, a sensor 182 for detecting one or more specific types of agents, elements, chemicals, compounds, etc., and a light alarm indicator 184. The sensor/detector 176 will be interconnected to the power source 174. In addition, mounted on and externally visible on the sides 168 or front 162 of the case 150 are a plurality of color coded indicator lights 186 with each light 186 corresponding to a specific agent, element, chemical, compound, etc., and lighting up when that agent is detected by the sensor/detector 176. The color coded indicator lights 186 will be electrically interconnected to the sensor/detectors 176 via any standard microprocessor. The cell phone detector case 150 and cell phone monitor 152 thus comprise a hand-held, easily portable and transportable detection means that is both effective and unobtrusive in its disposition and use.

FIGS. 18 and 19 illustrate representative examples of the integration of portable electronic communication or telecommuncation devices such as a cell phone 187*a* and/or a laptop computer 187*b* with the monitoring equipment 138 located at a predesignated monitoring site 188, and operating in conjunction with either a satellite and/or a cell phone tower 190 to transmit and receive signals and commands among each other and to a vehicle 192, such as a truck, as part of a stall-to-stop disabling system for slowing and stopping the vehicle 192 and locking a thief, terrorist, or unauthorized individual in the vehicle 192 if needed. A wide range of events can trigger and initiate the stall-to-stop system and the locking or lock disabling system and mechanism, and the event doesn't have to be limited to the detection of a bomb or a chemical, biological, or radiological agent, element, or compound. The events can include, but is not limited to, detection of an engine problem to engine failure to the unauthorized use (stealing) of the vehicle 192. The vehicle 192 includes an electromotive system 194 that comprises, among other components, an onboard computer(s), electrical, fuel and air systems, as well as brakes, ignition, steering, and transmission. Also integrated with and capable of communicating with the vehicle's 192 electromotive system 194 is a stall-to-stop system while a lock disabling mechanism 196 is able to engage and disengage or disable the vehicle's 192 locking mechanism 198 upon receipt of the appropriate commands via a lock disabling communication channel or link 200. This link 200 can also accommodate the stall-to-stop system commands and signals, and thus is a multi-channel communication link. A CPU or a transceiver 202 is programmed to receive signals from the cell phone tower 190 and/or to a GPS satellite 204 and is interconnected with the stall-to-stop system and the lock disabling system 196 via link 200 for engaging the electromotive system 194 and actuating the lock disabling system 196 to stop the vehicle 192 and lock inside the vehicle 192 anyone such as a thief, terrorist or other unauthorized individual.

A representative example for stopping, disabling, and locking the vehicle 192 that utilizes the cell phone tower 190 wherein the activation and/or distress signal 206 originates from the cell phone 187*a* or the laptop 187*b* and such activation signal 206 travels to the cell phone tower 190 that is nearest the current location of the vehicle 192. A signal 208 is then transmitted to the monitoring site 188 and specific monitoring equipment 138 that can also include but is not limited to cell phones, laptops, desktop PC's, notebook PC's and LCD monitors. The monitoring site 138 then communicates by signal 210 to the GPS satellite 204 that an original or activation signal has been received and then the GPS satellite 204 locates and communicates by multiplex signal 212 with the CPU or transceiver 202 on the vehicle 192 and exchanges information on the type of problem, situation, location, and vehicle speed. The monitoring equipment 138 then transmits a signal 214 to the cell phone tower 190 that communicates with the transceiver 202 and/or CPU of the vehicle 192 to initiate or execute any commands that will actuate the stall-to-stop disabling link 200 and lock disabling system 196 for bringing the vehicle 192 to a halt and actuating the vehicle's 192 locking mechanism 198 for locking the thief, terrorist, or other unauthorized person inside the vehicle 192 if needed.

FIG. 19 illustrates a representative example wherein the stall-to-stop system and the lock disabling system 196 are utilized in conjunction with the GPS satellite 204. In FIG. 19 a signal has traveled to the satellites nearest the vehicle's 192 current location and then the signal 218 has traveled to the monitoring equipment 138 and monitoring site 188 which can include but is not limited to satellite cell phones, satellite monitors, cell phones, laptops, desktop PC's, notebook PC's, and LCD monitors. The GPS satellite 204 then locates and communicates with the CPU and/or transceiver 202 on the vehicle 192 via a multiplex (two-way) signal 220 in order to exchange information on such distress and danger event parameters as the specific problem situation, location, and vehicle speed. The monitoring equipment 138 then transmits a signal 222 back to the GPS satellite 204 that in turn communicates via another signal 224 with the CPU and/or transceiver 202 to execute any commands to the stall-to-stop system for executing the disengagement of the vehicle's 192 electromotive system 194 for bringing the vehicle 192 to a halt and for actuating the lock disabling system 196 to direct the lock disabling link 200 to actuate the locking mechanism 198 thereby locking the vehicle 192 and anyone inside the vehicle 192.

The present invention comprehends a chemical/biological/radiological/nuclear/explosive/human/contraband detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars, United Parcel Services™ (UPS™), Federal Express™ (FedEx™), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans, unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and utility vehicles; the products grouped into what may be referred to as Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, door sensors, speed sensors, biometric sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems, detection of humans, detection of contraband, temperature, and shock levels; the products grouped into what may be referred to as Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, eyeglass, briefcases, detector cases of locks, detector cases of tags, detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to; the products grouped into what may be referred to as Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, web servers, desktop personal computers (PCs), notebook personal computers (PCs), laptops, satellite cell phones, cell phones, Universal Mobile Telecommunications System (UMTS) phones, personal digital assistants (PDAs), liquid crystal display (LCD) monitors, and satellite monitoring, remote control key fobs, two-way communication key fobs, handhelds; the products grouped into what may be referred to as Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), General Packet Radio Services (GPRS), Global System for Mobile (GSM), Wideband Code Division Multiple Access (W-CDMA), Universal Mobile Telecommunications System (UMTS), Short Message Service (SMS); the products grouped into what may be referred to as Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature. the products grouped into what may be referred to as Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside or outside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

While the invention has been shown and described in a preferred embodiment, it will be apparent to those skilled in the art that numerous alterations, modifications, and variations will possible and practicable without departing from the spirit and scope of the invention as set forth by the appended claims.

What is claimed:

1. Monitoring equipment that is at least one of products grouped together by common features of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to a lock for communication therebetween; the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;

a transmitter for transmitting signals and messages to at least one of a remote lock, an electrical lock, a mechanical lock, or automatic lock;

a receiver for receiving signals from at least one of a remote lock, an electrical lock, a mechanical lock, or automatic lock;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;

a short-range radio frequency (RF) connection that is near-field communication (NFC);

at least one of the satellite connection, Bluetooth connection, WiFi connection, Internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver,

at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and

the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a remote lock, an electrical lock, a mechanical lock, or automatic lock, whereupon a signal is sent to the receiver of the monitoring equipment from at least one of the remote lock, electrical lock, mechanical lock, or automatic lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.

2. Monitoring equipment that is at least one of products grouped together by common features of a computer terminal, person computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to at least one of a home lock, a building lock, or a cargo container lock for communication therebetween; the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;

a transmitter for transmitting signals and messages to at least one of a home lock, a building lock, or a cargo container lock;

a receiver for receiving signals from at least one of a home lock, a building lock, or a cargo container lock;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;

a short-range radio frequency (RE) connection that is near-field communication (NFC);

at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RE) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver;

at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and

the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a home lock, a building lock, or a cargo container lock whereupon a signal is sent to the receiver of the monitoring equipment from at least one of the home lock, building lock, or cargo container lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.

3. Monitoring equipment that is at least one of products grouped together by common features of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal, digital assistant (PDA) or smart phone interconnected to a vehicle lock for communication therebetween; the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;

a transmitter for transmitting signals and messages to at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock;

a receiver for receiving signals from at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;

a short-range radio frequency (RF) connection that is near-field communication (NFC);

at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver;

at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and

the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock, whereupon a signal is sent to the receiver of the monitoring equipment from at least one of the manned or unmanned aerial vehicle lock, manned or unmanned ground vehicle lock, or manned or unmanned sea vehicle lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.

4. A communication device comprising:

at least one central processing unit (CPU);

at least one motion sensor in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

at least one biometric sensor in communication with the at least one CPU for providing biometric authentication to access the communication device;

at least one or more detectors in communication with the art least one CPU for detecting at least one of a chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.

5. A monitoring device, comprising:

at least one central processing unit (CPU);

at least one temperature sensor in communication with the at least one CPU for monitoring temperature;

at least one motion sensor in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;

at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;

one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.

6. A monitoring equipment, comprising:

at least one central processing unit (CPU);

at least one motion sensor in communication with the at least one CPU;

at least one light indicator in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

at least one biometric sensor in communication with the at least one CPU for providing biometric authentication to access the communication device;

at least one or more detectors in communication with the art least one CPU for detecting at least one of a chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.

* * * * *

Exhibit D

DEFENSE THREAT REDUCTION AGENCY

BROAD AGENCY ANNOUNCEMENT

HDTRA1-19-S-0005

BAA Call CBI-01

CHEMICAL / BIOLOGICAL TECHNOLOGIES

May 7, 2019

1.0 Purpose

This is a BAA Call to RD-CB BAA HDTRA1-19-S-0005. The purpose of this BAA Call is to request proposals for Topic CBI-01 "Chemical and Biological Threats: TAK Plugins for Warning & Reporting and Decision Making".

2.0 Topic Description

2.1 Background

Mobile applications are revolutionizing the way we approach new technologies for the Department of Defense (DoD). Lightweight and transportable devices such as smartphones and tablets have demonstrated their potential to change the way we approach decision support capabilities that enable the Warfighter to operate under the threat of Chemical and Biological threats. Already, systems such as Nett Warrior have deployed under wartime conditions, increasing situational awareness, decreasing reaction and decision times, and augmenting operational capability. The Tactical Assault Kit (TAK)—a mapping system with a plugin architecture—has seen similar success across the DoD and DHS, where operators must routinely execute missions in spectrum denied environments. Three iterations of TAK are of interest: ATAK (Android OS), WinTAK (Microsoft Windows OS), and WebTAK (web browser based). At present, ATAK has over 40,000 DoD users. Past demonstrations of the ATAK system includes the proven ability to promulgate situational awareness in network permissive environments and the ability to effectively and efficiently collaborate and allocate resources and personnel critical to the mission. The Chemical and Biological Defense Program charges the Joint Science and Technology Office (JSTO) Digital Battlespace Management Division with researching and developing technologies to support the warfighter. JSTO develops tools to generate decision-oriented information and enable enhanced situational awareness with the goal of protecting military and civilian populations from intentional or incidental chemical or biological threats and Toxic Industrial Chemicals/Materials (TIC/TIM) hazards.

2.2 Objective

This topic supports the development of ATAK, WinTAK, and WebTAK compatible versions of existing decision support tools for chemical and biological warning and reporting, hazard prediction, and consequence assessment. Given that our warfighters must operate in environments with little to no network connectivity, proposed software applications should be able to operate both with network connectivity and without. Proposals should leverage existing tools, DoD or otherwise, implement an agile development approach with multiple releases, and deliver a final product running in multiple TAK architectures within 12 months of award.

2.3 Software Considerations

Successful efforts will provide:

- Software that is fully documented and easy to access, modify, and extend (modular)
- Application with a robust data management approach, supporting easy retrieval/sending of updated data sources in a connected state and efficient storage of necessary data, on the device, for use during disconnected operations.
- Software that is able to comply with DoD standards for authorization to operate
- Software that is tested and verified
- User Interface Designs that consider the warfighter (e.g., impact of PPE, voice activation)

2.4 Impact

This topic will ultimately support the warfighters ability to operate in and overcome a chemical or biological threat environment through the effective promulgation of situational awareness information and the use of superior tactical decision-making tools.

2.5 References

Department of Defense. (2004). Chemical, Biological, Radiological, and Nuclear Defense Program: Report to Congress. Washington, D. C.: DoD.

Department of Defense. (2008). DoD CBRN Defense: Doctrine, Training, Leadership, and Education Strategic Plan. Washington, D. C.: CBDP.

Department of Defense. (2018). Joint Electronic Library. Washington, D.C.: DoD. Accessed at: http://www.jcs.mil/Doctrine/

Joint Acquisition CBRNE Knowledge System (2018). JACKS: News and Application Console. Retrieved from JACKS: https://pki.jacks.jpeocbd.army.mil

Joint Publication 3-41, CBRNE Response

Joint publication 3-11, Operations in CBRNE Environments

Low, Cherlynn. What do made for AI processors really do? (2017) Accessed at: https://www.engadget.com/2017/12/15/ai-processor-cpu-explainer-bionic-neural-npu/

National Academy of Sciences. (1999). Philosophy, Doctrine, and Training for Chemical and Biological Warfare. Retrieved from Strategies to Protect the Health of Deployed U.S. Forces: Force Protection and Decontamination: https://www.ncbi.nlm.nih.gov/books/NBK225131/

US Army (2018). "CBRN Force Modernization Strategy."

3.0 Communications

3.1 Questions about this BAA Call

Questions regarding the technical and administrative content of this BAA Call must be sent to the following DTRA e-mail address: dtra.belvoir.rd.mbx.rd-cb-baa-with-calls@mail.mil. All questions must include the BAA Call number in the subject line (i.e. HDTRA1-19-S-0005 BAA Call CBI-01). The deadline to submit questions is 2:00pm EDT on May 17, 2019.

3.2 Communication Guidelines Prior to Receipt of a Proposal

DTRA supports technical dialogue between the Science and Technology Manager (STM) and proposers after release of this BAA Call and prior to the receipt of proposals. All technical inquiries shall be submitted to the BAA e-mail box (refer to Section 3.1) and/or at the Proposer's Day event (refer to Section 3.4). Attempts to contact the PM through methods other than the BAA e-mail box and/or attendance at the Proposer's Day event will be disregarded. Technical dialogue may occur by e-mail, phone or in-person. General guidelines for dialogue between the STM and proposers prior to receipt of a proposal include the following:

- The STM will not be obligated by any discussion with a potential proposer. Communications between the STM and potential proposer shall not constitute a commitment by the Government to subsequently fund or award any proposed effort.

- The STM cannot attempt to replace the potential proposer's original ideas with his or her own ideas.

- The STM cannot share ideas, technical solutions or proprietary information that were provided to him or her by another potential proposer.

- If the STM provides information concerning the objectives/goals/requirements of the BAA to one proposer, he or she must provide this information to all proposers. Similarly, if a proposer is provided information that expands on information contained in the published solicitation or is otherwise publically available, it must also be made publically available to all potential proposers. Answers to questions concerning objectives, goals, or requirements of this BAA Call will be shared with all proposers and posted to the FedBizOpps (FBO) website. It is the proposer's responsibility to periodically check the FBO website to view postings of questions and answers, in addition to any applicable amendments to the BAA Call.

- Potential proposers may submit an inquiry to verify interest in the effort to be proposed prior to committing any resources to the preparation of any proposals in response to this BAA Call. Notwithstanding the Government's response, all eligible sources may submit a proposal to this BAA Call.

3.3 Communication Guidelines after Receipt of a Proposal

The Government reserves the right to engage in communications with proposers during the course of evaluations for the purpose of enhancing the Government's understanding of a research proposal and facilitating the evaluation process. These communications may be executed via email or teleconference, and the information obtained may be considered in rating proposals.

The primary focus of these communications is to address any proposal ambiguity that may preclude the evaluation of the merits of a proposal. Accordingly, the Government's decision to engage in communications with a proposer will be on a case by case basis, as needed to facilitate the evaluation process. These communications will not be utilized as an opportunity for proposers to alter any aspect of their proposal, or to address identified weaknesses or deficiencies within the proposal.

3.4 Proposer's Day

The Government plans to host a Proposers Day event on June 4, 2019. The details of this event to include registration requirements and agenda can be found here: https://cvent.me/vPAoL. Attendance at the Proposer's Day is voluntary and is not required in order to propose to this BAA Call.

4.0 Proposal Submission Deadline

The proposal submission deadline is June 24, 2019 at 2:00pm EDT. Proposals must be received by this time and date in order to be considered. Submission information is provided in Section 6.0 of this Call.

5.0 Instructions to Proposers

To assure timely and equitable evaluation of proposals, Proposers must follow the instructions contained herein. Proposers are required to meet all solicitation requirements, including terms and conditions, representations and certifications, technical requirements, and proposal content and format requirements. Failure to meet a requirement may result in an offer being ineligible for award. Additionally, Proposers must clearly identify any exception to the solicitation terms and conditions and provide complete accompanying rationale. It is the Proposer's responsibility to ensure the completeness of the proposal. Evaluation of a proposal will be conducted only on the basis of the information contained within it and the Government will not assume that a Proposer possesses any capabilities not specified.

Proposals shall be clear, concise, and include sufficient detail for effective evaluation and for substantiating the validity of stated claims. The Proposer shall assume that the Government has no prior knowledge of the Proposer's capabilities.

6.0 Proposal Submission Instructions

6.1 General Instructions

All proposals must be submitted electronically through the DTRA proposal submission website: http://www.dtrasubmission.net. Any proposal submitted by any means other than the DTRA proposal submission website **will not** be considered (e.g., hand-carried, postal service, commercial carrier, e-mail).

Proposers are responsible for ensuring submission of their proposals by the date and time specified in Section 4.0. **Time management is wholly the responsibility of the Proposer. If a timely submission is not fully uploaded prior to the cutoff date/time, the proposal will not be considered. No exceptions will be made.** The Proposer must verify the submission of their proposal package by printing the electronic receipt (time and date stamped) that appears on the final screen following compliant submission of a proposal to the DTRA proposal submission website.

Using the DTRA proposal submission website, all Proposers must prepare Proposal Cover Sheets for each proposal submitted. All data point requirements must be completed in every cover sheet. Once the cover sheet is saved, the system will assign a unique proposal number for each submission. Cover sheets may be edited as often as necessary until the submission period closes. All submissions must be dated and **unclassified.**

If multiple proposals are being submitted by the same Proposer in response to this Topic, separate cover sheets must be generated for each proposal and the full proposal files must be uploaded with the associated cover sheet, since a unique document number will automatically be assigned to each submission by the electronic proposal tracking system. All documents submitted to the DTRA proposal submission website are considered works in progress and are not eligible for evaluation until the Proposer submits the final proposal package for consideration. Once all proposal files have been uploaded and the Proposer is ready to submit their application, select the green "Submit" button on the page. A confirmation message will appear on the page once the submission has gone through. Perform a virus check before uploading any proposal files. If a virus is detected, it may cause rejection of the file.

Proposers **must** submit proposals to the appropriate BAA Call and Topic. Failure to do so will render the proposal ineligible for evaluation and award.

6.2 Late Submissions and Withdrawal of Proposals

Proposers are responsible for access to the DTRA proposal submission website and for submitting electronic proposals so as to be received at the Government site indicated in this BAA Call no later than the closing date and time stated in Section 4.0, above. Untimely proposals will not be considered.

When sending electronic files, the Proposer will account for potential delays in file transfer from the originator's computer server to the Government website/computer server. Proposers are encouraged to submit their proposals early to avoid potential file transfer delays due to high demand or problems encountered in the course of the submission. Proposers should also print, and maintain for their records, the electronic date/time stamped receipt that appears on the final screen following submission of a proposal on the DTRA proposal submission website. All submissions shall be fully uploaded before the cut off time/date in order to be considered.

Proposals may be withdrawn by written notice received at any time before award. Withdrawals are effective upon receipt of notice via the e-mail address listed in Section 3.0.

6.3 Proposal Format Requirements

6.3.1 Submission File Format

Proposers shall submit the required components of each proposal volume as specified below.

6.3.1.1 Technical Volume

- Technical Proposal – Portable Document Format (PDF) compatible with Adobe Acrobat ® version 11.0.0 or earlier.
- Draft Statement of Work (SOW) – MS Word

6.3.1.2 Cost Volume

- Rough Order of Magnitude (ROM) Cost Spreadsheet – MS Excel

6.3.1.3 Supplemental Information Volume

- Supplemental Information Coversheet – PDF compatible with Adobe Acrobat ® version 11.0.0 or earlier.

Additional specific format requirements are provided below. Movie and sound file attachments, or other additional files, will not be accepted. The proposal files must not be encrypted.

6.3.2 Proposal Format Requirements

Proposers submitting proposals must follow the instructions provided in this section of the BAA Call; failure to do so may preclude consideration of the proposal for award. Proposals shall conform to the following format requirements.

6.3.2.1 Technical Volume

6.3.2.1.1 Technical Proposal

- Paper size: 8.5 x 11 inches
- Spacing: Single-spaced
- Margins: One-inch
- Font: Times New Roman, not smaller than 12 point
- Page Limit: No more than ten (10) pages. Pages in excess of the page limitation will not be read or evaluated.
- Classification: Unclassified
- Restrictive Markings: Documents containing proprietary information shall contain the restrictive markings reflected in Section 6.3.3.

6.3.2.1.2 Draft SOW

- Paper size: 8.5 x 11 inches
- Spacing: Single-spaced
- Margins: One-inch
- Font: Times New Roman, not smaller than 12 point
- Page Limit: None. Further, the SoW will not count against the 10-page Technical Proposal page limit.
- Classification: Unclassified
- Restrictive Markings: The draft SOW must not contain information deemed trade secret, confidential or proprietary by the Proposer or Contractor- specific references such as headers and footers with company name and/or logo. See Attachment 1 for more information.

6.3.2.2 Cost Volume

6.3.2.2.1 ROM Cost Spreadsheet

- File Format: MS Excel 2013, or compatible format
- Format: In accordance with Attachment 2
- Formulas: All formulas shall be preserved.
- Page Limit: None
- Classification: Unclassified
- Restrictive Markings: Documents containing proprietary information shall contain the restrictive markings reflected in Section 6.3.3.

6.3.2.3 Supplemental Information Volume

- File Format: PDF compatible with Adobe Acrobat ® version 11.0 or earlier
- Format: In accordance with Attachment 4
- Page Limit: None
- Classification: Unclassified
- Restrictive Markings: Documents containing proprietary information shall contain the restrictive markings reflected in Section 6.3.3.

6.3.3 Restrictive Markings and Disclosure of Proprietary Information

Proposal content submitted in response to this BAA Call (with the exception of the SOW) may contain technical information and other data that the Proposer does not want disclosed to the public or used by the Government for any purpose other than proposal evaluation. Public release of information in any submission will be subject to existing statutory and regulatory requirements. If proprietary information which constitutes a trade secret, proprietary commercial or financial information, confidential personal information, or data affecting national security is provided by a Proposer, it will be treated in confidence, to the extent permitted by law, provided that the following legend appears and is completed on the front of the submission:

> "For any purpose other than to evaluate the white proposal, this data shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed in whole or in part, provided that, if an award is made to the Proposer as a result of or in connection with the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the agreement. This restriction does not limit the right of the Government to use information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is contained in page(s) of this proposal."

Any other legend may be unacceptable to the Government and may constitute grounds for removing the proposal from further consideration without assuming any liability for inadvertent disclosure. The Government will limit dissemination of properly marked information to official channels.

In addition, the pages indicated as restricted must be marked with the following legend: "Use or disclosure of the white paper/proposal data on lines identified by an asterisk (*) are subject to the restriction on the front page of this proposal." The Government assumes no liability for disclosure or use of unmarked data and may use or disclose such data for any purpose."

In the event that properly marked data contained in a proposal submitted in response to this BAA Call is requested pursuant to the Freedom of Information Act, 5 U.S.C. § 552, the Proposer will be advised of such request and, prior to such release of information, will be requested to expeditiously submit to DTRA a detailed listing of all information in the white proposal which the Proposer believes to be exempt from disclosure under the Act. Such action and cooperation on the part of the Proposer will ensure that any information released by DTRA pursuant to the Act is properly identified.

By submission of a proposal, the Proposer understands that proprietary information may be disclosed outside the Government for the sole purpose of technical evaluation. The Contracts Office will obtain a written agreement from the evaluator that proprietary information in the proposal will only be used for evaluation purposes and will not be further disclosed or utilized.

6.4 Proposal Content Requirements

Proposers must follow the instructions provided in this section of the BAA Call; failure to do so may preclude consideration of the proposal for award. All proposals shall consist of a Technical Volume and Cost Volume conforming to the following content requirements:

6.4.1 Technical Volume

The Technical Volume shall be comprised of a Technical Proposal, consisting of a Technical Section, a Project Management Section and a draft SOW, conforming to the following requirements:

6.4.1.1 Technical Section

The Technical Section shall be submitted in accordance with the following:

A. Technical Approach. Proposers shall describe in detail the proposed technical approach. Within the technical approach narrative, Proposers shall address the items contained within the "Software Considerations" section of the Topic.

B. Relevance. Proposers shall describe the relevance of the proposed project in terms of end-user needs. Focus should include how the proposed technology will impact the end user and provide increased capability over the current capability.

6.4.1.2 Project Management Section

Proposers shall provide a project management plan, their capabilities to perform the proposed work, and a Gantt chart.

A. Project Management Plan. Proposers shall describe their project management plan for the proposed project. The Proposer shall address each of the following:

1. Explain how the Proposers will manage the project, ensuring that the required performance outcomes are achieved within the required schedule, at or below the contract cost ceiling.

2. Provide the processes and techniques that demonstrate the Proposer's ability to act as a resource integrator with the capability to effectively manage all aspects of execution of the technical approach, to include:

   a) Identifying and addressing project technical risk;
   b) Leveraging and managing resident expertise, teaming arrangements and/or other partnerships to provide the required capabilities to successfully execute the technical approach and accomplish the tasks identified in the Statement of Work;
   c) Effectively and efficiently managing and leading assigned tasks, including those assigned to external organizations; and
   d) Identifying key personnel to include a Program/Project Manager responsible for providing cohesive technical and administrative leadership and direction to facilitate the successful completion of contract requirements.

3. Explain the risks associated with achieving proposed project goals, objectives and milestones (what will be done), and risks associated with the technical approach (how it will be done). For all identified risks, Proposers shall indicate how they plan to manage these risks (e.g. avoidance, acceptance, mitigation, transfer) and provide a detailed narrative explaining the corresponding risk management actions that will be taken for each identified risk.

B. Gantt Chart. Proposers shall provide a Gantt chart that lists each individual SOW task and provides the duration of performance for each, and incorporates proposed development milestones. The Gantt chart will not count toward the 10-page technical proposal page limitation.

6.4.1.3 Draft Statement of Work

The draft SOW shall be submitted in accordance with the sample template provided in Attachment 1. The draft SOW will not count toward the 10-page technical proposal page limitation.

6.4.2 Supplemental Information Volume

Proposers shall provide the following information as part of the Supplemental Information Volume:

A. Supplemental Information Cover Sheet. Proposers shall provide a Supplemental

Information Cover Sheet in accordance with Attachment 4.

B. Intellectual Property.

1. Patents - Proposers must list any known patents, patent applications, or inventions which the Proposer may be required to license in order to perform the work described in the Proposer's proposal, or which the Government may be required to license to make or use the deliverables of the contract should the Proposer's proposal be selected for award. For any patent or patent application listed above, the Proposer must provide the patent number or patent application publication number, a summary of the patent or invention title, and indicate whether the Proposer is the patent or invention owner. If a patent or invention is in-licensed by the Proposer, identify the licensor.

   If any listed patent, patent application or invention is owned or licensed by the Proposer, the Proposer must provide a statement, in writing, if it either owns or possesses the appropriate licensing rights to patent, patent application or invention to perform the work described in the proposal and/or to grant the Government a license to make or use the deliverables for this program. If any listed patent, patent application or invention is not owned or licensed by the Proposer, then the Proposer must explain how it will obtain a license, how the Government may obtain a license and/or whether the Proposer plans to obtain these rights on behalf of the Government.

   Be advised that no patent, patent application or invention disclosure will be accepted if identified in the Data Rights Assertion list described below under "Data Rights". Existing inventions, patents and patent applications should be discussed in the above list. Government rights in any technology that might be invented or reduced to practice under the contract are addressed in the patent rights clause to be included in the contract.

2. Data Rights - Proposals submitted in response to this BAA Call shall identify, to the extent known at the time an offer is submitted to the Government, the technical data or computer software that the Proposer, its subcontractors or suppliers, or potential subcontractors or suppliers, assert should be furnished to the Government with restrictions on use, release, or disclosure, in accordance with DFARS 252.227-7017, Identification and Assertion of Use, Release or Disclosure Restrictions, and DFARS 252.227-7028, Technical Data or Computer Software Previously Delivered to the Government. The Proposer's assertions, including the assertions of its subcontractors or suppliers or potential subcontractors or suppliers, shall be submitted as an attachment to its offer, utilizing Attachment 3 – Data Rights Assertion List, dated and signed by an official authorized to contractually obligate the Proposer. If

the Proposer will deliver all technical data and computer software to the Government without restrictions, enter "NONE" in this table under the heading "Technical Data or Computer Software to be Furnished with Restrictions." Proposers responding to this BAA Call requesting an OTA shall specifically identify any asserted restrictions on the Government's use of intellectual property contemplated under those award instruments. For this purpose, Proposers must propose specific Intellectual Property terms and conditions and a data deliverable list. Proposers are encouraged to model their data rights assertions list to the template provided in DFARS 252.227-7017.

C. Conflict of Interest. Certain post-employment restrictions on former federal officers and employees may exist, including special Government employees (including but not limited to Section 207 of Title 18, United States Code, the Procurement Integrity Act, 41 U.S.C. 423, and FAR 3.104). If a prospective Proposer believes that a conflict of interest exists that relates to the above restrictions, the situation should be raised to the DTRA Contracting Officer before time and effort are expended in preparing a proposal. Send notification of potential conflict of interest via an e-mail message to the e-mailbox listed in Section 3.0 of this BAA Call.

All Proposers and proposed subcontractors also must affirmatively disclose whether or not they are providing scientific, engineering and technical assistance (SETA), A&AS or similar support, through an active contract or subcontract, to any DTRA technical office(s), the Joint Program Executive Office for Chemical and Biological Defense (JPEO), Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ATSD-NCB), or the Office of the Special Assistant for Chemical and Biological Defense and Chemical Demilitarization Programs (OSA(CBD&CDP)). All disclosures must state which office(s) the Proposer supports, and identify the prime contract number. Disclosures must be furnished at the time of proposal submission. All facts relevant to the existence or potential existence of organizational conflicts of interest (FAR 9.5) must be disclosed, including facts not specifically described above. The disclosure must include a description of the action the Proposer has taken or proposes to take to avoid, neutralize, or mitigate such conflict.

D. DoD Laboratory and Federally Funded Research and Development Centers (FFRDC). Proposed collaboration with a DoD laboratory should be clearly identified in the proposal, and must be supported with a letter of intent from the laboratory's Commander.

DoD-sponsored FFRDs should review DFARS 235.017 to ensure compliance with the requirement for a DoD-approved conflict of interest policy.

In accordance with FAR 17.503(e), DoE Order 481.1E and DoE Acquisition Regulation DEARS 970.1707-3, DoE FFRDC participants must provide a copy of the written certification from the DoE sponsor authorizing its performance of the proposed effort. The DoE sponsor must provide written certification that the proposed work: (1) is consistent with or complimentary to missions of DoE and the facility to which the work is to be assigned; (2) will not adversely impact programs assigned to the facility; and (3) will not create a detrimental future burden on DoE resources.

In accordance with FAR 17.503(e), 35.017(a)(2) and 35.017-3, FFRDC participants (other than DoE FFRDCs) must provide documentation from the FFRDC sponsor authorizing its performance of the proposed effort.

E. Export Control Notification. Proposers are responsible for ensuring compliance with all export control laws and regulations that may be applicable to the export of and foreign access to their proposed technologies. Proposers may consult with the Department of State with any questions regarding the International Traffic in Arms Regulation (ITAR) (22CFR Parts 120 – 130) and/or the Department of Commerce regarding the Export Administration Regulations (EAR) (15 CFR Parts 730-774). The Department of State publishes guidance on the ITAR at http://www.pmddtc.state.gov. Department of Commerce guidance on the EAR is located at http://www.bis.doc.gov.

6.4.3 Cost Volume

Proposers shall prepare the ROM utilizing Attachment 2 – ROM Cost Spreadsheet. The ROM is in excel format. Proposers shall follow all instructions, including provided Notes, contained within the ROM Cost Spreadsheet.

7.0 Evaluation Criteria

7.1 General Evaluation Information

Evaluation of proposals will be conducted based upon a technical subject matter expert review as described in FAR Subparts 6.102(d)(2) and 35.016. Each proposal will be evaluated based on the merit and relevance of the specific proposal as it relates to the DTRA program rather than against other proposals for research in the topic area. All documents necessary for the review and evaluation of proposal submissions must be provided as described in Section 6 of this BAA Call.

7.2 Adjectival Ratings

The Government will evaluate proposals using the adjectival ratings below. Proposers are advised that a strength is an aspect of a proposal that has merit or exceeds specified performance or capability requirement in a way that will be advantageous to the Government during contract performance. A weakness means a flaw in the proposal that increases the risk of unsuccessful contract performance. A deficiency is a material failure of a proposal to meet a Government requirement or a combination of significant weaknesses in a proposal that increases the risk of unsuccessful contract performance to an unacceptable level.

Rating	Description
Outstanding (O)	The proposal is a technically exceptional submission that is pertinent to program goals and objectives. The proposal contains multiple strengths that will provide significant benefit to the Government, and that far outweigh any weaknesses. The risk of unsuccessful performance is low.
Good (G)	The proposal is a technically thorough submission that is pertinent to program goals, and objectives. The proposal contains at least one strength that will provide benefit to the Government, and that outweighs any weaknesses. The risk of unsuccessful performance is low to moderate.
Acceptable (A)	The proposal is a technically adequate submission that is pertinent to program goals, and objectives. Strengths and weaknesses are offsetting or will have little or no impact on contract performance. The risk of unsuccessful performance is no worse than moderate.
Marginal (M)	The proposal is a technically weak submission that is pertinent to program goals, and objectives. The proposal has one or more weaknesses which are not offset by strengths. The risk of unsuccessful performance is high.
Unacceptable (U)	The proposal does not meet requirements, or is not pertinent to program goals and objectives and contains one or more deficiencies. The proposal is unawardable.

7.3 Evaluation of Proposals

The evaluation of proposals will be accomplished through a technical peer review of each proposal in accordance with the evaluation criteria listed in order of relative importance, below. Each criterion will be assigned one of the following adjectival ratings: Outstanding (O), Good (G), Acceptable (A), Marginal (M) or Unacceptable (U). Any factor scored as "Unacceptable (U)" will render the Proposer's proposal "Unawardable," and the proposal will not be considered further.

7.3.1 Criterion 1 –Technical Approach

Reviewers will assess the extent to which the Proposer has proposed a comprehensive and sound technical approach that addresses the software considerations contained within the Section 2.3 of the Topic. It should be noted that while Reviewers will assess proposals against all items contained within Section 2.3, the following considerations are deemed to be of the highest importance:

- The extent to which the proposed approach results in software that is fully documented and easy to access, modify and extend (modular);
- the extent to which the proposed approach results in software that is tested and verified; and
- the extent to which the proposed approach results in software that incorporates user interface designs that consider the warfighter (e.g. impact of PPE, voice activation).

Additionally, it should be noted that proposals that demonstrate the following may be evaluated more favorably.

- A clear technical approach for developing segmented, but multi-purpose, code to allow deployment to different architectures (e.g. ATAK, WinTAK, and WebTAK);
- An approach that provides for software with Government Purpose Rights that does not require recurring license fees; and
- Utilization of an Agile development framework that allows for iterative software builds and continuous end user feedback.

Finally, Reviewers will assess the extent to which the proposed technology addresses end user needs, is relevant to current CBDP priorities, and represents improvement over current chemical and biological technology capability.

7.3.2 Criterion 2 –Project Management

Reviewers will assess the extent to which the Proposer has proposed a sound project management plan, and has assembled the requisite expertise and skills to successfully perform the proposed project. It should be noted that while Reviewers will assess proposals based on the merit of the provided project management plan and the demonstrated capability to perform the proposed scope of work proposals that demonstrate the following capability may be evaluated more favorably.

- Familiarity with the TAK infrastructure and capability to provide tool demos within the TAK Server and ATAK environments.

While no cost-related evaluation criteria will be utilized in the review of proposals, the information contained within the ROM Cost Spreadsheet will be assessed by Reviewers primarily for the purpose of determining the ability to fund all or part of the proposed project. However, it should be noted that the ROM Cost Spreadsheet may be considered during the review of the technical proposal, particularly in cases where the information contained in the cost submission casts significant doubt on 1) the validity of the proposed technical and/or program management approach, and/or 2) the Proposer's capability to execute the proposed scope of work. In such cases, the relevant evaluation findings will be addressed within the narratives of the relevant criterion.

8.0 Selection Decision Information

Proposers shall refer to Section 6.0 of the Baseline BAA for selection decision information.

9.0 Post-Selection Activities

Proposers shall refer to Section 7.0 of the Baseline BAA for information regarding post-selection activities.

10.0 Applicability of Baseline BAA

All requirements of HDTRA1-19-S-0005 apply unless specifically amended and addressed in this BAA Call. For complete information regarding HDTRA1-19-S-0005, refer to the baseline BAA in FedBizOpps. It contains information applicable to all BAA Calls issued under the BAA and provides information on the overall program, proposal preparation and submission requirements, proposal review and evaluation criteria, selection, post-selection activities, etc. Please direct questions to the e-mail box identified in Section 3.1.

11.0 List of Attachments

ATTACHMENT 1:	Statement of Work Template
ATTACHMENT 2:	ROM – Cost Spreadsheet
ATTACHMENT 3:	Data Rights Assertion List
ATTACHMENT 4:	Supplemental Information Coversheet

Exhibit E

United States Court of Appeals for the Federal Circuit

LARRY GOLDEN,
Plaintiff-Appellant

v.

GOOGLE LLC,
Defendant

2022-1267

Appeal from the United States District Court for the District of South Carolina in No. 6:21-cv-00244-JD, Judge Joseph Dawson, III.

JUDGMENT

THIS CAUSE having been considered, it is

ORDERED AND ADJUDGED:

VACATED AND REMANDED

FOR THE COURT

September 8, 2022
Date

/s/ Peter R. Marksteiner
Peter R. Marksteiner
Clerk of Court

NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

LARRY GOLDEN,
Plaintiff-Appellant

v.

APPLE INC., SAMSUNG ELECTRONICS USA, LG ELECTRONICS USA, INC., QUALCOMM INCORPORATED, MOTOROLA SOLUTIONS, INC., PANASONIC CORPORATION, AT&T INC., VERIZON CORPORATION SERVICE GROUP, SPRINT CORPORATION, T-MOBILE USA, INC., FORD GLOBAL TECHNOLOGIES, LLC, FAIRWAY FORD LINCOLN OF GREENVILLE, GENERAL MOTORS COMPANY, KEVIN WHITAKER CHEVROLET, FCA US LLC, BIG O DODGE CHRYSLER JEEP RAM,
Defendants

2022-1229

Appeal from the United States District Court for the District of South Carolina in No. 6:20-cv-04353-JD, Judge Joseph Dawson, III.

LARRY GOLDEN,
Plaintiff-Appellant

v.

GOOGLE LLC,
Defendant

2022-1267

Appeal from the United States District Court for the District of South Carolina in No. 6:21-cv-00244-JD, Judge Joseph Dawson, III.

Decided: September 8, 2022

LARRY GOLDEN, Greenville, SC, pro se.

Before DYK, TARANTO, and STOLL, *Circuit Judges.*

PER CURIAM

Larry Golden appeals two orders of the United States District Court for the District of South Carolina ("district court") dismissing his patent infringement claims against various defendants. We *affirm* the dismissal in Case No. 22-1229 but *vacate* the dismissal in Case No. 22-1267 and *remand* for further proceedings consistent with this opinion.

BACKGROUND

Mr. Golden owns a family of patents concerning a system for locking, unlocking, or disabling a lock upon the detection of chemical, radiological, and biological hazards.[1] In 2019, he sued sixteen defendants in the district court, alleging patent infringement by their development and manufacturing of certain devices. The district court dismissed the suit without prejudice, and this court affirmed the dismissal "on the ground of frivolousness" because Mr. Golden's complaint "offer[ed] only vague generalities and block quotes of statutes, cases and treatises, but nowhere point[ed] us to any nonfrivolous allegations of infringement of any claim by any actual product made, used, or sold by any defendant." *Golden v. Apple Inc.*, 819 F. App'x 930, 931 (Fed. Cir. 2020).

On January 5, 2021, in Case No. 22-1229, Mr. Golden again sued the same sixteen defendants from the 2019 case for patent infringement ("the Apple case"). He initially filed the same over-300-page complaint held to be frivolous in the 2019 case. After the magistrate judge imposed a 35 page limit on the complaint, Mr. Golden filed a shortened complaint complying with the restriction. On January 26, 2021, in Case No. 22-1267, Mr. Golden separately sued Google LLC for patent infringement ("the Google case"). The magistrate judge reviewed the complaints in both cases and recommended summary dismissal with prejudice without issuance of service of process or leave to amend and monetary sanctions for the filing of frivolous litigation.

In both cases, the district court adopted the magistrate judge's recommendations in part. In the Apple case, the district court dismissed the complaint as frivolous without the issuance of service of process but declined to dismiss with prejudice. Additionally, the district court lifted the page restriction for an amended complaint. In the Google case, the district court dismissed the complaint with

[1] The patents at issue in these cases are U.S. Patent Nos. 7,385,497; 9,096,189; 9,589,439; 10,163,287 and Reissue Patent Nos. RE43,891 and RE43,990.

prejudice and without the issuance of service of process. Mr. Golden appeals the district court decisions in both cases. We have jurisdiction under 28 U.S.C. § 1295(a)(1). On appeal, Mr. Golden has filed briefs, while the defendants have not filed responsive briefs.

DISCUSSION

Under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), a court must dismiss a complaint if it fails to allege "enough facts to state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570. This standard "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* at 555 (citation omitted). A plaintiff must allege facts that give rise to "more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678 (citation omitted). In the patent context, this court has explained that a plaintiff need not "plead facts establishing that each element of an asserted claim is met," *In re Bill of Lading Transmission and Processing Sys. Pat. Litig.*, 681 F.3d 1323, 1335 (Fed. Cir. 2012) (citing *McZeal v. Sprint Nextel Corp.*, 501 F.3d 1354, 1357 (Fed. Cir. 2007)), but must plead "'enough fact[s] to raise a reasonable expectation that discovery will reveal' that the defendant is liable for the misconduct alleged." *Id.* at 1341 (alteration in original) (quoting *Twombly*, 550 U.S. at 556). We review the district court's dismissal of the complaint de novo. *Anand v. Ocwen Loan Servicing, LLC*, 754 F.3d 195, 198 (4th Cir. 2014).

In the Apple case, the district court dismissed the docketed complaint as frivolous after finding that Mr. Golden "failed to include factual allegations beyond the identities of the Defendants, reference to the alleged infringing devices, and the alleged infringed-upon patents." Dist. Ct. Op. at 4–5. We agree with the district court: the docketed complaint is nothing more than a list of patent claims and accused products manufactured by each defendant for each asserted patent. Mr. Golden contends that his original complaint contained sufficient factual allegations to support his claims. However, he concedes that the rejected original complaint was identical to the one that this court deemed frivolous in the 2019 case. His effort to relitigate the sufficiency of the original complaint is precluded under the doctrine of res judicata. *See Arizona v. California*, 530 U.S. 392, 412 (2000) ("[I]f a court is on notice that it has previously decided the issue presented, the court may dismiss the action *sua sponte*, even though [a preclusion] defense has not been raised."). Mr. Golden does not argue that the docketed complaint contains factual allegations beyond those contained in his original complaint or that the allegations in the docketed complaint do anything beyond listing the alleged infringed-upon patent claims and the alleged infringing devices. This is plainly insufficient. We see no error in the district court's without prejudice dismissal of the Apple case.

In the Google case, the district court again concluded that Mr. Golden's complaint was frivolous. Here, however, Mr. Golden's complaint includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189. The district court discounted this claim chart because it "contains the exact same language as the claim charts previously rejected by the Federal Circuit [in the 2019 case], although Google Pixel 5 Smartphone appears in the far left column instead of Apple." Dist. Ct. Op. at 4. But to the extent that the chart includes the "exact same language" as previously rejected charts, it is simply the language of the independent claims being mapped to. The key column describing the infringing nature of the accused products is not the same as the complaint held frivolous in the 2019 case. It attempts—whether successfully or not—to map claim limitations to infringing product features, and it does so in a relatively straightforward manner.

We conclude that the district court's decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart. On remand, the district court should allow the complaint to be filed and request service of process. Our decision does not preclude subsequent motions to dismiss by the defendant for failure to state a claim or for summary judgment. We express no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous.

CONCLUSION

For the foregoing reasons, we affirm the district court's dismissal in Case No. 22-1229, vacate the dismissal in Case No. 22-1267, and remand for further proceedings consistent with this opinion.

CASE NO. 22-1229 AFFIRMED

CASE NO. 22-1267 VACATED AND REMANDED

COSTS

No costs.